(12)特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2005 年8 月18 日 (18.08.2005)

PCT

(10) 国際公開番号
WO 2005/076142 A1

(51) 国際特許分類[7]: G06F 12/14, 15/00, G11B 20/10, H04L 9/32

(21) 国際出願番号: PCT/JP2005/000497

(22) 国際出願日: 2005 年1 月17 日 (17.01.2005)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願2004-027940 2004 年2 月4 日 (04.02.2004) JP

(71) 出願人 (米国を除く全ての指定国について): ソニー株式会社 (SONY CORPORATION) [JP/JP]; 〒1410001 東京都品川区北品川６丁目７番３５号 Tokyo (JP).

(72) 発明者; および

(75) 発明者/出願人 (米国についてのみ): 浅野 智之 (ASANO, Tomoyuki) [JP/JP]; 〒1410001 東京都品川区北品川６丁目７番３５号 ソニー株式会社内 Tokyo (JP).

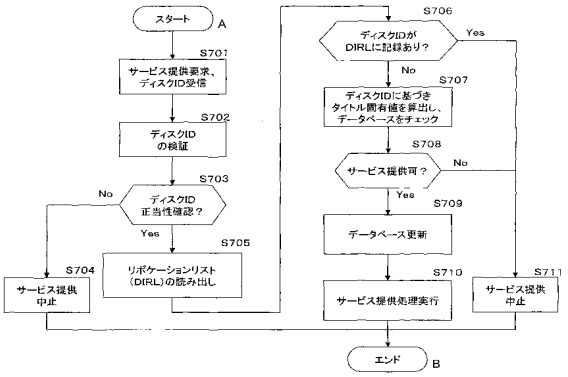
(74) 代理人: 宮田 正昭, 外(MIYATA, Masaaki et al.); 〒1040041 東京都中央区新富一丁目１番７号 銀座ティーケイビル 澤田・宮田・山田特許事務所 Tokyo (JP).

(81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT,

[続葉有]

(54) Title: SERVICE PROVIDING SERVER, INFORMATION PROCESSOR, DATA PROCESSING METHOD, AND COMMUTER PROGRAM

(54) 発明の名称: サービス提供サーバ、情報処理装置、およびデータ処理方法、並びにコンピュータ・プログラム



A- START
S701- REQUEST SERVICE PROVISION AND RECEIVE DISK ID
S702-CHECK DISK ID
S703- DISK ID AUTHENTICATION ASCERTAINED?
S704- STOP SERVICE PROVISION
S705 -READ REVOCATION LIST (DIRL)
S706 -DISK ID RECORDED IN DIRL?
S707- COMPUTE TITLE CHARACTERISTIC VALUE ACCORDING TO DISK ID AND CHECK DATABASE
S708- CAN SERVICE BE PROVIDED?
S709- UPDATE DATABASE
S710- PROVIDE SERVICE
S711- STOP SERVICE PROVISION
B- END

(57) Abstract: A device and method for providing service corresponding to the content stored in an information recording medium only to a device having an authentic information recording medium. A content stored in an information recording medium is provided, and service from a service providing server connected to a network is provided. The service providing server checks the information recording medium ID sent from a user device, judges from service providing state data on each information recording medium ID whether service can be provided or not, and provides the service. Only when the information processor that has sent a service request has read the authentic information recording medium ID from an information recording medium and is allowed to receive service according to the service providing state data, the service is provided.

(57) 要約: 情報記録媒体に格納したコンテンツに対応したサービスの提供を正当な情報記録媒体を持つデバイスに対してのみ実行することを可能とした装置、方法を提供する。情報記録媒体にコンテンツを格納して提供し、さらにネットワーク接続したサービス提供サーバからのサービス提供処理を行なう構成において、サービス提供サーバがユーザデバイスから送信される情報記録媒体ＩＤを検証し、情報記録媒体ＩＤ毎のサービス提供状況データに基づいてサービス提供可否を判定してサービス提供を行なう。サービス要求を送信した情報処理装置が正当な情報記録媒体ＩＤを情報

[続葉有]

WO 2005/076142 A1

LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) 指定国 (表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:
— 国際調査報告書

２文字コード及び他の略語については、定期発行される各*PCT*ガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

明 細 書

サービス提供サーバ、情報処理装置、およびデータ処理方法、並びにコンピュータ・プログラム

技術分野

[0001] 本発明は、サービス提供サーバ、情報処理装置、およびデータ処理方法、並びにコンピュータ・プログラムに関する。詳細には、コンテンツを格納したディスクなどの情報記録媒体の再生処理を実行するユーザデバイスに対して、コンテンツに関するサービスの提供を実現するサービス提供サーバ、情報処理装置、およびデータ処理方法、並びにコンピュータ・プログラムに関する。

背景技術

[0002] 音楽等のオーディオデータ、映画等の画像データ、ゲームプログラム、各種アプリケーションプログラム等、様々なソフトウエアデータ(以下、これらをコンテンツ(Content)と呼ぶ)は、記録メディア、例えば、DVD(Digital Versatile Disc)、MD(Mini Disc)、CD(Compact Disc)、あるいは青色レーザを利用した高密度記録可能なディスク[青色光ディスク(Blu-ray Disc)]などの情報記録媒体に格納されてユーザに提供され、ユーザは、PC(Personal Computer)、ディスクプレーヤ等のユーザデバイス、すなわち再生装置においてコンテンツを再生し利用することができる。

[0003] さらに、近年、ディスク等の情報記録媒体に格納されたコンテンツに関連する様々なサービスを、ユーザデバイスとネットワーク接続したサーバから提供するサービス提供構成が利用されている。

[0004] 例えば、ディスク格納コンテンツが外国語映画である場合の音声に対する字幕データや吹き替え音声データ、あるいはコンテンツの続編のディスクの購入割引券など、様々なコンテンツ関連サービスが、ネットワークを介して接続したサーバからPC等のユーザデバイスに提供される。

[0005] サーバから提供するサービスの形体は、様々であり、ユーザの制限を設けることのないサービス形態もあるが、例えばサービス関連コンテンツを記録したディスク1枚につき1度までなど、一定の条件下でのサービス提供形態もある。

[0006] ディスクに格納されるコンテンツ、すなわち、音楽データ、画像データ等、多くのコンテンツは、一般的にその作成者あるいは販売者に頒布権等が保有され、これらのコンテンツの利用については一定の利用制限、すなわち、正規なユーザに対してのみ、コンテンツの利用を許諾し、許可のない利用が行われないようにする構成をとるのが一般的となっている。

[0007] 従って、コンテンツに関連して提供するサービスについても、一定の利用権限の確認、例えば、正規ディスクの購入ユーザであることの確認処理などを条件としてサービス提供を許容するといったシステムの構築が望まれている。

発明の開示

発明が解決しようとする課題

[0008] 本発明は、上述の問題点に鑑みてなされたものであり、DVD、CD、青色レーザ記録媒体等の各種情報記録媒体にコンテンツを格納して提供し、さらにネットワーク接続したサービス提供サーバからのサービス提供処理を行なう構成において、正当なサービス利用権限を確認して、不正なサービス利用を排除することを可能とするサービス提供サーバ、情報処理装置、およびデータ処理方法、並びにコンピュータ・プログラムを提供することを目的とする。

課題を解決するための手段

[0009] 本発明の第1の側面は、

情報処理装置からのサービス提供要求に応じたサービス提供処理を実行するサービス提供サーバであり、

情報処理装置からの情報記録媒体IDおよびサービスIDを伴うサービス要求を受信するデータ受信部と、

情報記録媒体の格納コンテンツのタイトルに対応するタイトル固有値毎のサービス管理データとして前記情報記録媒体ID毎のサービス提供状況データを格納した記憶部と、

前記データ受信部を介して受信した情報記録媒体IDの検証処理を実行し、正当性が確認されたことを条件として、該情報記録媒体IDに基づいてタイトル固有値を取得し、タイトル固有値に対応するサービス提供状況データを前記記憶部から取得し

て、前記情報記録媒体IDおよび前記サービスIDによって特定されるサービスの提供可否を判定し、提供可能であるとの判定を条件としたサービス提供処理を実行するデータ処理部と、

を有することを特徴とするサービス提供サーバにある。

[0010] さらに、本発明のサービス提供サーバの一実施態様において、前記データ処理部は、情報記録媒体IDの検証処理を情報記録媒体IDに含まれる署名データの検証処理として実行し、情報記録媒体IDに含まれるタイトル固有値、または情報記録媒体IDに含まれるデータに基づく演算を実行して算出したタイトル固有値に従って、タイトル固有値対応のサービス提供状況データを前記記憶部から取得する処理を実行する構成であることを特徴とする。

[0011] さらに、本発明のサービス提供サーバの一実施態様において、前記サービス提供サーバは、不正な情報記録媒体IDのリストであるリボケーションリストを格納した記憶部を有し、前記データ処理部における情報記録媒体IDの検証処理は、情報処理装置から受信した情報記録媒体IDと、前記リボケーションリストに記録されたIDとの照合処理として実行することを特徴とする。

[0012] さらに、本発明のサービス提供サーバの一実施態様において、前記情報記録媒体IDは、情報記録媒体の格納コンテンツのタイトルに対応するタイトル固有値と、管理装置の秘密鍵に基づいて生成された情報記録媒体毎に異なる署名データとを含み、前記データ処理部は、前記情報記録媒体IDの検証処理を、前記情報記録媒体IDに含まれる署名データに対する前記管理装置の公開鍵を適用したメッセージ生成および照合処理として実行するとともに、情報記録媒体IDに含まれるタイトル固有値に対応するサービス提供状況データを前記記憶部から取得する処理を実行する構成であることを特徴とする。

[0013] さらに、本発明のサービス提供サーバの一実施態様において、前記情報記録媒体IDは、製造された情報記録媒体の枚数Wに対応して設定される素数p(w)と、素数p(w)と、タイトル固有値に基づく演算によって算出されるデータIDKey(w)とを含み、前記データ処理部は、前記情報記録媒体IDに含まれるデータが素数であるか否かを判定する処理をID検証処理として実行するとともに、情報記録媒体IDに含まれる

データIDKey(w)からタイトル固有値を算出し、算出したタイトル固有値に対応するサービス提供状況データを前記記憶部から取得する処理を実行する構成であることを特徴とする。

[0014] さらに、本発明の第2の側面は、

サービス提供サーバに対するサービス提供要求を実行する情報処理装置であり、

情報記録媒体のアクセス処理を実行する記録媒体インタフェースと、

前記記録媒体インタフェースを介して情報記録媒体から読み取られた情報記録媒体IDの検証処理を実行し、正当性が確認されたことを条件として、該情報記録媒体IDのサービス提供サーバに対する送信処理を実行するデータ処理部と、

を有することを特徴とする情報処理装置にある。

[0015] さらに、本発明の情報処理装置の一実施態様において、前記データ処理部は、情報記録媒体IDの検証処理を、情報記録媒体IDに含まれる署名データの検証処理として実行する構成であることを特徴とする。

[0016] さらに、本発明の情報処理装置の一実施態様において、前記データ処理部における情報記録媒体IDの検証処理は、不正な情報記録媒体IDのリストであるリボケーションリストを記憶部または情報記録媒体から取得し、取得したリボケーションリストに記録されたIDと、情報処理装置から受信した情報記録媒体IDとの照合処理として実行する構成であることを特徴とする。

[0017] さらに、本発明の情報処理装置の一実施態様において、前記情報記録媒体IDは、情報記録媒体の格納コンテンツのタイトルに対応するタイトル固有値と、管理装置の秘密鍵に基づいて生成された情報記録媒体毎に異なる署名データとを含み、前記データ処理部は、前記情報記録媒体IDの検証処理を、前記情報記録媒体IDに含まれる署名データに対する前記管理装置の公開鍵を適用したメッセージ生成および照合処理として実行する構成であることを特徴とする。

[0018] さらに、本発明の情報処理装置の一実施態様において、前記情報記録媒体IDは、製造された情報記録媒体の枚数Wに対応して設定される素数p(w)と、素数p(w)と、タイトル固有値に基づく演算によって算出されるデータIDKey(w)とを含み、前記データ処理部は、前記情報記録媒体IDに含まれるデータが素数であるか否かを

判定する処理をID検証処理として実行する構成であることを特徴とする。

[0019] さらに、本発明の第3の側面は、

情報処理装置からのサービス提供要求に応じた処理を実行するデータ処理方法であり、

情報処理装置からの情報記録媒体IDおよびサービスIDを伴うサービス要求を受信するデータ受信ステップと、

受信した情報記録媒体IDの検証処理を実行し、正当性が確認されたことを条件として、該情報記録媒体IDに基づいてタイトル固有値を取得し、情報記録媒体の格納コンテンツのタイトルに対応するタイトル固有値毎のサービス管理データとして前記情報記録媒体ID毎のサービス提供状況データを格納した記憶部から、取得したタイトル固有値に対応するサービス提供状況データを取得して、前記情報記録媒体IDおよび前記サービスIDによって特定されるサービスの提供可否を判定し、提供可能であるとの判定を条件としたサービス提供処理を実行するデータ処理ステップと、

を有することを特徴とするデータ処理方法にある。

[0020] さらに、本発明のデータ処理方法の一実施態様において、前記データ処理ステップは、情報記録媒体IDの検証処理を情報記録媒体IDに含まれる署名データの検証処理として実行し、情報記録媒体IDに含まれるタイトル固有値、または情報記録媒体IDに含まれるデータに基づく演算を実行して算出したタイトル固有値に従って、タイトル固有値対応のサービス提供状況データを前記記憶部から取得する処理を実行するステップを含むことを特徴とする。

[0021] さらに、本発明のデータ処理方法の一実施態様において、前記データ処理ステップにおける情報記録媒体IDの検証処理は、情報処理装置から受信した情報記録媒体IDと、不正な情報記録媒体IDのリストであるリボケーションリストに記録されたIDとの照合処理として実行するステップを含むことを特徴とする。

[0022] さらに、本発明のデータ処理方法の一実施態様において、前記情報記録媒体IDは、情報記録媒体の格納コンテンツのタイトルに対応するタイトル固有値と、管理装置の秘密鍵に基づいて生成された情報記録媒体毎に異なる署名データとを含み、前記データ処理ステップは、前記情報記録媒体IDの検証処理を、前記情報記録媒

体IDに含まれる署名データに対する前記管理装置の公開鍵を適用したメッセージ生成および照合処理として実行するとともに、情報記録媒体IDに含まれるタイトル固有値に対応するサービス提供状況データを前記記憶部から取得する処理を実行するステップを含むことを特徴とする。

[0023] さらに、本発明のデータ処理方法の一実施態様において、前記情報記録媒体IDは、製造された情報記録媒体の枚数Wに対応して設定される素数p(w)と、素数p(w)と、タイトル固有値に基づく演算によって算出されるデータIDKey(w)とを含み、前記データ処理ステップは、前記情報記録媒体IDに含まれるデータが素数であるか否かを判定する処理をID検証処理として実行するとともに、情報記録媒体IDに含まれるデータIDKey(w)からタイトル固有値を算出し、算出したタイトル固有値に対応するサービス提供状況データを前記記憶部から取得する処理を実行するステップを含むことを特徴とする。

[0024] さらに、本発明の第4の側面は、

サービス提供サーバに対するサービス提供要求を実行するデータ処理方法であり、

記録媒体インタフェースを介して情報記録媒体のアクセス処理を実行する情報記録媒体アクセスステップと、

前記記録媒体インタフェースを介して情報記録媒体から読み取られた情報記録媒体IDの検証処理を実行し、正当性が確認されたことを条件として、該情報記録媒体IDのサービス提供サーバに対する送信処理を実行するデータ処理ステップと、

を有することを特徴とするデータ処理方法にある。

[0025] さらに、本発明のデータ処理方法の一実施態様において、前記データ処理ステップは、情報記録媒体IDの検証処理を、情報記録媒体IDに含まれる署名データの検証処理として実行することを特徴とする。

[0026] さらに、本発明のデータ処理方法の一実施態様において、前記データ処理ステップにおける情報記録媒体IDの検証処理は、不正な情報記録媒体IDのリストであるリボケーションリストを記憶部または情報記録媒体から取得し、取得したリボケーションリストに記録されたIDと、情報処理装置から受信した情報記録媒体IDとの照合処理と

して実行するステップを含むことを特徴とする。

[0027] さらに、本発明のデータ処理方法の一実施態様において、前記情報記録媒体IDは、情報記録媒体の格納コンテンツのタイトルに対応するタイトル固有値と、管理装置の秘密鍵に基づいて生成された情報記録媒体毎に異なる署名データとを含み、前記データ処理ステップは、前記情報記録媒体IDの検証処理を、前記情報記録媒体IDに含まれる署名データに対する前記管理装置の公開鍵を適用したメッセージ生成および照合処理として実行するステップを含むことを特徴とする。

[0028] さらに、本発明のデータ処理方法の一実施態様において、前記情報記録媒体IDは、製造された情報記録媒体の枚数Wに対応して設定される素数p(w)と、素数p(w)と、タイトル固有値に基づく演算によって算出されるデータIDKey(w)とを含み、前記データ処理ステップは、前記情報記録媒体IDに含まれるデータが素数であるか否かを判定する処理をID検証処理として実行するステップを含むことを特徴とする。

[0029] さらに、本発明の第5の側面は、

情報処理装置からのサービス提供要求に応じた処理を実行するコンピュータ・プログラムであり、

情報処理装置からの情報記録媒体IDおよびサービスIDを伴うサービス要求を受信するデータ受信ステップと、

受信した情報記録媒体IDの検証処理を実行し、正当性が確認されたことを条件として、該情報記録媒体IDに基づいてタイトル固有値を取得し、情報記録媒体の格納コンテンツのタイトルに対応するタイトル固有値毎のサービス管理データとして前記情報記録媒体ID毎のサービス提供状況データを格納した記憶部から、取得したタイトル固有値に対応するサービス提供状況データを取得して、前記情報記録媒体IDおよび前記サービスIDによって特定されるサービスの提供可否を判定し、提供可能であるとの判定を条件としたサービス提供処理を実行するデータ処理ステップと、

を有することを特徴とするコンピュータ・プログラムにある。

[0030] さらに、本発明の第6の側面は、

サービス提供サーバに対するサービス提供要求を実行するコンピュータ・プログラムであり、

記録媒体インタフェースを介して情報記録媒体のアクセス処理を実行する情報記録媒体アクセスステップと、

前記記録媒体インタフェースを介して情報記録媒体から読み取られた情報記録媒体IDの検証処理を実行し、正当性が確認されたことを条件として、該情報記録媒体IDのサービス提供サーバに対する送信処理を実行するデータ処理ステップと、

を有することを特徴とするコンピュータ・プログラムにある。

[0031] なお、本発明のコンピュータ・プログラムは、例えば、様々なプログラム・コードを実行可能なコンピュータ・システムに対して、コンピュータ可読な形式で提供する記憶媒体、通信媒体、例えば、CDやFD、MOなどの記録媒体、あるいは、ネットワークなどの通信媒体によって提供可能なコンピュータ・プログラムである。このようなプログラムをコンピュータ可読な形式で提供することにより、コンピュータ・システム上でプログラムに応じた処理が実現される。

[0032] 本発明のさらに他の目的、特徴や利点は、後述する本発明の実施例や添付する図面に基づくより詳細な説明によって明らかになるであろう。なお、本明細書においてシステムとは、複数の装置の論理的集合構成であり、各構成の装置が同一筐体内にあるものには限らない。

発明の効果

[0033] 本発明の構成によれば、DVD、CD、青色レーザ記録媒体等の各種情報記録媒体にコンテンツを格納して提供し、さらにネットワーク接続したサービス提供サーバからのサービス提供処理を行なう構成において、サービス提供サーバ側において、情報処理装置(ユーザデバイス)から送信される情報記録媒体IDを検証し、情報記録媒体ID毎のサービス提供状況データに基づくサービス提供を行なう構成としたので、サービス要求を送信した情報処理装置が正当な情報記録媒体IDを情報記録媒体から読み取った情報処理装置であり、サービス提供状況データに基づいてサービス提供が許容されているサービスであることが確認された場合に限り、サービスの提供が実行される。

[0034] さらに、本発明の構成によれば、情報記録媒体に格納された情報記録媒体IDは、管理装置の署名データなどの正当性の確認可能なデータを含み、また、タイトル固

有値を有するかあるいは算出可能なデータを含む構成としたので、サービス提供サーバにおいては、情報記録媒体IDに含まれるデータに基づく正当性の確認が可能であり、また、タイトル固有値を取得することが可能となり、タイトル固有値に対応付けて設定されたサービス提供状況データの特定を行なうことが可能となる。

図面の簡単な説明

[0035] [図1]情報記録媒体の格納データを説明する図である。

[図2]リボケーションリストの構成について説明する図である。

[図3]メッセージ認証コード(MAC:Message Authentication Code)を用いた際のMAC生成、検証処理について説明する図である。

[図4]各種キー、データの暗号化処理、配布処理に適用される階層型木構造を説明する図である。

[図5]コンテンツ鍵の有効化キーブロック(EKB)を使用した配布例と復号処理例を示す図である。

[図6]情報記録媒体の製造、管理処理構成について説明する図である。

[図7]サービス提供サーバの構成例について説明する図である。

[図8]サービス提供サーバの保有するサービス提供状況データを示す図である。

[図9]情報処理装置(ユーザデバイス)の構成例について説明する図である。

[図10]ディスクIDの設定例について説明する図である。

[図11]情報処理装置(ユーザデバイス)の実行する処理を説明するフローチャートである。

[図12]情報処理装置(ユーザデバイス)の実行するディスクID検証シーケンスを説明するフローチャートである。

[図13]情報処理装置(ユーザデバイス)の実行するディスクID検証シーケンスを説明するフローチャートである。

[図14]情報処理装置(ユーザデバイス)の実行するディスクID検証シーケンスを説明するフローチャートである。

[図15]情報処理装置(ユーザデバイス)の実行するディスクID検証シーケンスを説明するフローチャートである。

[図16]情報処理装置(ユーザデバイス)がサービス提供サーバからサービスを受領する処理について説明する図である。

[図17]サービス提供サーバの実行する処理を説明するフローチャートである。

発明を実施するための最良の形態

[0036] 以下、図面を参照しながら本発明のサービス提供サーバ、情報処理装置、およびデータ処理方法、並びにコンピュータ・プログラムの詳細について説明する。なお、説明は、以下の項目に従って行なう。

1. 情報記録媒体の格納データ
2. コンテンツ格納情報記録媒体の提供および利用管理構成
3. サービス提供サーバおよびユーザデバイスを構成する情報処理装置の構成
4. ユーザデバイスにおける処理の詳細
5. サービス提供サーバにおける処理の詳細

[0037] [1. 情報記録媒体の格納データ]

図1に情報記録媒体のデータ記録構成例を示す。図1は、CD(Compact Disc)、DVD(Digital Versatile Disc)、MD(Mini Disc)、青色光ディスク(Blu-ray Disc)、フラッシュメモリ等、各種の情報記録媒体100の格納データについて説明する図である。図1にはディスク状の媒体を例として示してあるが、本発明はディスク状の媒体に限らず、フラッシュメモリ等の各種の情報記録媒体において適用可能である。

[0038] 情報記録媒体100には、図1に示す情報、すなわち、ディスクID101、コンテンツ102、ディスクIDリボケーションリスト(DIRL:Disc ID Revocation List)103、暗号鍵情報(EKB:Enabling Key Block)104が格納されている。

[0039] ディスクID101は例えばディスク固有の識別子であり、消去や書き換えが困難であるように格納される。なお、本発明において、ディスクID101は、情報記録媒体100に格納されるコンテンツ102に対応するタイトルごとに固有の値(タイトル固有値)と、情報記録媒体100ごとに固有の値(ディスク固有値)と、その正当性を示す情報、例えば署名などの情報(正当性検証値)などにより構成される。ディスクIDの詳細については、後述する。

[0040] なお、以下に説明する実施例では、ディスク状の媒体をコンテンツ格納情報記録媒

体の例として示しているので、その識別子をディスクIDとして説明する。フラッシュメモリ等の各種の情報記録媒体をコンテンツ格納情報記録媒体として利用した場合はディスクIDに対応する情報記録媒体IDが設定される。

[0041] 情報記録媒体100には、さらに、コンテンツ102が格納される。コンテンツは例えば暗号化コンテンツとして格納される。暗号化コンテンツとした場合は、コンテンツを復号するための鍵情報が、情報記録媒体100に格納されるか、あるいはネットワークを介して提供される。

[0042] 情報記録媒体100には、さらにディスクIDリボケーションリスト(DIRL:Disc ID Revocation List)103が格納される。ディスクIDリボケーションリスト(DIRL:Disc ID Revocation List)103は、不正コピー等が行われたと認定されたディスク、例えば市場に不正なコピーコンテンツを格納したCD−Rが発見された場合に、その不正CD−RにコンテンツとともにコピーされたディスクIDを抽出し、リスト化したデータである。ディスクIDリボケーションリスト(DIRL:Disc ID Revocation List)103の生成、管理、ディスク製造者に対するリスト情報の提供などは、特定の信頼される管理局(CA:Central Authority)が実行する。

[0043] ディスクIDリボケーションリスト(DIRL:Disc ID Revocation List)のデータ構成について、図2を参照して説明する。ディスクIDリボケーションリスト(DIRL:Disc ID Revocation List)150は、図2に示すように、リスト(DIRL:Disc ID Revocation List)が作成された時期により単調増加するバージョン番号151と、排除すべきディスクのディスクIDを羅列したリボークディスクIDリスト152と、バージョン番号151とリボークディスクIDリスト152に対する改竄検証値153としての認証子が含まれる。改竄検証値153は、対象となるデータ、この場合はバージョン番号151とリボークディスクIDリスト152が改竄されているか否かを判別するために適用するデータであり、公開鍵暗号技術を用いたデジタル署名や、共通鍵暗号技術を用いたメッセージ認証コード(MAC:Message Authentication Code)が適用される。

[0044] 改竄検証値153として公開鍵暗号技術を用いたデジタル署名を用いる際には、信頼できる機関、例えば上述の管理局(CA:Central Authority)の署名検証鍵(公開鍵)を再生機が取得し、管理局(CA:Central Authority)の署名生成鍵(秘密鍵)を用い

て作られた署名を各再生機が取得した署名検証鍵(公開鍵)によって検証することで、バージョン番号151とリボークディスクIDリスト152が改竄されているか否かを判別する。

[0045] 改竄検証値153としてメッセージ認証コード(MAC:Message Authentication Code)を用いた際のMAC生成、検証処理について、図3を参照して説明する。メッセージ認証コード(MAC:Message Authentication Code)は、データの改竄検証用のデータとして生成されるものであり、MAC生成処理、検証処理態様には様々な態様が可能であるが、1例としてDES暗号処理構成を用いたMAC値生成例を図3に示す。

[0046] 図3に示すように、対象となるメッセージ、この場合は、図2に示すバージョン番号151とリボークディスクIDリスト152を8バイト単位に分割し、(以下、分割されたメッセージをM1、M2、・・・、MNとする)、まず、初期値(Initial Value(以下、IVとする))とM1を排他的論理和する(その結果をI1とする)。次に、I1をDES暗号化部に入れ、鍵(以下、K1とする)を用いて暗号化する(出力をE1とする)。続けて、E1およびM2を排他的論理和し、その出力I2をDES暗号化部へ入れ、鍵K1を用いて暗号化する(出力E2)。以下、これを繰り返し、全てのメッセージに対して暗号化処理を施す。最後に出てきたENがメッセージ認証符号(MAC(Message Authentication Code))となる。

[0047] MAC値は、その生成元データが変更されると、異なる値となり、検証対象のデータ(メッセージ)に基づいて生成したMACと、記録されているMACとの比較を行い、一致していれば、検証対象のデータ(メッセージ)は変更、改竄がなされていないことが証明される。

[0048] 図1に戻り、情報記録媒体100の格納データについての説明を続ける。情報記録媒体100には、さらに暗号鍵情報(EKB:Enabling Key Block)104が格納されている。

[0049] 暗号鍵情報(EKB)を利用した秘密情報提供構成について、図を参照して説明する。図4の最下段に示すナンバ0ー15が、例えばコンテンツ利用を行なう情報処理装置としてのユーザデバイスである。すなわち図4に示す階層ツリー(木)構造の各葉(リーフ:leaf)がそれぞれのデバイスに相当する。

[0050] 各デバイス0ー15は、製造時あるいは出荷時、あるいはその後において、階層ツリー（木）構造における自分のリーフからルートに至るまでのノードに割り当てられた鍵（ノードキー）および各リーフのリーフキーからなるキーセット（デバイスキー（DNK：Device Node Key））をメモリに格納する。図4の最下段に示すK0000ーK1111が各デバイス0ー15にそれぞれ割り当てられたリーフキーであり、最上段のKR（ルートキー）から、最下段から2番目の節（ノード）に記載されたキー：KRーK111をノードキーとする。

[0051] 図4に示す木構造において、例えばデバイス0はリーフキーK0000と、ノードキー：K000、K00、K0、KRをデバイスキーとして所有する。デバイス5はK0101、K010、K01、K0、KRを所有する。デバイス15は、K1111、K111、K11、K1、KRを所有する。なお、図4のツリーにはデバイスが0ー15の16個のみ記載され、ツリー構造も4段構成の均衡のとれた左右対称構成として示しているが、さらに多くのデバイスがツリー中に構成され、また、ツリーの各部において異なる段数構成を持つことが可能である。

[0052] また、図4のツリー構造に含まれる各デバイスには、様々な記録媒体、例えば、デバイス埋め込み型あるいはデバイスに着脱自在に構成されたDVD、CD、MD、フラッシュメモリ等を使用する様々なタイプのデバイスが含まれている。さらに、様々なアプリケーションサービスが共存可能である。このような異なるデバイス、異なるアプリケーションの共存構成の上に図4に示すコンテンツあるいは鍵配布構成である階層ツリー構造が適用される。

[0053] これらの様々なデバイス、アプリケーションが共存するシステムにおいて、例えば図4の点線で囲んだ部分、すなわちデバイス0，1，2，3を1つのグループとして設定する。例えば、この点線で囲んだグループ内に含まれるデバイスのみが情報記録媒体に格納した暗号化コンテンツの正当な利用権、すなわちライセンスを保有する。この場合、デバイス0，1，2，3のみがコンテンツ復号に適用する鍵の取得を可能としたEKBを設定して、暗号化コンテンツを格納した情報記録媒体に格納することになる。

[0054] 図4から明らかなように、1つのグループに含まれる3つのデバイス0，1，2，3はそれぞれのデバイスに格納したデバイスキー（DNK：Device Node Key）として共通のキ

ーK00、K0、KRを保有している。

[0055] このとき、デバイス0，1，2のみがコンテンツの復号に適用するコンテンツキーKconを取得可能としたEKBの構成は、例えば図5に示す構成となる。すなわち、EKBは、

インデックス 暗号化データ

000 Enc(K000, Kcon)

0010 Enc(K0010, Kcon)

として設定される。

[0056] なお、Enc(Kx, Ky)は、データKyを鍵Kxで暗号化した暗号化データを意味する。このとき、デバイス0，1は自己の保有するデバイスキー[K000]を用いてインデックス[000]の暗号化データの復号が可能であり、またデバイス2はデバイスキー[K0010]を用いて上記EKBのうちのインデックス[0010]の暗号化データの復号が可能であり、それぞれの暗号化データの復号処理によりコンテンツキーKconを取得することができる。その他のデバイスは、デバイスキー[K000]、[K0010]のいずれも保有しておらず、図5に示す構成を持つEKBを受領してもEKBの復号によるコンテンツキーの取得ができない。

[0057] このように、EKBは、ライセンスを保有するデバイスに応じた構成データとすることで、任意の選択されたデバイスにおいてのみ処理可能としてコンテンツ鍵等の秘密情報を特定のデバイスにのみ提供可能とした鍵情報ブロックとして構成される。鍵情報(EKB)発行センタ104は、コンテンツの利用を許容するデバイスにおいてのみ処理可能なEKBを生成して情報記録媒体製造エンティティ103に提供する。情報記録媒体製造エンティティ103はこのEKBを暗号化コンテンツとともに情報記録媒体110に格納してユーザに提供する。

[0058] [2. コンテンツ格納情報記録媒体の提供および利用管理構成]

図6は、上述の各種データを格納した情報記録媒体200の提供および利用管理構成を説明する図である。

[0059] 図6に示すように、コンテンツ提供および管理構成においては、管理局(CA:Central Authority)が使用する管理装置201と、コンテンツプロバイダが使用するコンテンツ提供装置203と、ディスク製造者が使用するディスク製造装置202と、ユーザ

が使用するコンテンツ再生処理を行なう情報処理装置（ユーザデバイス）400と、情報処理装置（ユーザデバイス）400に対して情報記録媒体200に格納されたコンテンツに対応するサービス、例えば字幕情報の提供処理などを実行するサービス提供サーバ300が存在する。

[0060] 管理装置201が、前述したディスクIDとディスクIDリボケーションリスト（DIRL）とを生成してディスク製造装置202に提供する。また、コンテンツ提供装置203が、暗号化コンテンツと有効化鍵ブロック（EKB）とをディスク製造装置202に提供する。

[0061] ディスク製造装置202は、管理装置201から受けたディスクIDおよびディスクIDリボケーションリスト（DIRL）と、コンテンツ提供装置203から受けた暗号化コンテンツデータと有効化鍵ブロック（EKB）とを記録した情報記録媒体200を製造する。

[0062] ユーザは、情報記録媒体200を例えば購入し、情報処理装置（ユーザデバイス）400にセットする。情報処理装置（ユーザデバイス）400は、情報記録媒体200に記録されたディスクIDが正当であると検証し、当該ディスクIDがリボケーションリストDIRL内に存在しないことを確認し、自らのデバイスノード鍵データDNKに基づいて有効化鍵ブロックEKBから適切なコンテンツ鍵データを取得し、暗号化コンテンツデータを復号し、再生することができる。

[0063] さらに、情報処理装置（ユーザデバイス）400は、情報記録媒体200に記録されたディスクIDと、サービス識別子としてのサービスIDをサービス提供サーバ300に送信し、サービス提供サーバ300において、ディスクIDの正当性が検証され、さらにサービスの提供の可否をサービス提供サーバ300の有するサービス提供状況データに基づいて判定し、ディスクIDが正当であり、サービス提供状況データに基づいてサービス提供可能と判定した場合に、情報処理装置（ユーザデバイス）400に対するサービス提供処理を実行する。

[0064] ［3．サービス提供サーバおよびユーザデバイスを構成する情報処理装置の構成］

次に、サービス提供サーバおよびユーザデバイスを構成する情報処理装置の構成について説明する。

[0065] 図7は、図6に示すサービス提供サーバの構成図である。図7に示すように、サービ

ス提供サーバ300は、例えば、CPU等によって構成されるコントローラ302、各種の演算処理を実行する演算ユニット303、データ入力装置やデータ出力装置に対するデータ入出力、およびネットワークを介するデータ入出力用のインタフェースとしての入出力インタフェース(I／F)304、セキュアメモリ305、メインメモリ306を有する。これらはバス301を介して接続されている。

[0066] メインメモリ306は、演算ユニット303およびコントローラ302における処理に用いられる種々のデータのうち、セキュリティレベルが低いデータを記憶する。セキュアメモリ305は、演算ユニット303およびコントローラ302の処理に用いられる種々のデータのうち、セキュリティレベルが高いデータを記憶する。セキュアメモリ305は、例えば、図6に示す管理装置201から受領するディスクIDなどを記憶する。

[0067] 入出力インタフェース304は、例えば、図示しない操作手段あるいはネットワークなどに接続され、図6に示す管理装置201や、コンテンツ提供装置203からの様々なデータの受領を行い、また、サービス提供を受ける情報処理装置(ユーザデバイス)400との通信を実行してサービスを提供する。

[0068] 演算ユニット303は、コントローラ302からの制御に基づいて、署名データの検証用データの生成など、各種の演算を実行する。コントローラ302は、例えばユーザデバイスに対するサービス提供を許容してよいか否かの確認処理プログラム、サービス提供プログラムなどの各種のプログラムを実行する。

[0069] サービス提供サーバ300は、入出力インタフェース(I／F)304を介して、管理装置201またはコンテンツ提供装置203またはその他の装置からディスクIDリボケーションリストを定期的に、またはイベントごとに受信し、常に最新版をセキュアメモリ305に格納する。

[0070] また、入出力インタフェース(I／F)304を介して、コンテンツ提供装置203またはその他の装置から、タイトルごとのタイトル固有値と、提供するサービスを識別するサービス識別情報を受信し、タイトルごとのサービス提供状況情報を管理したサービス提供状況データベースをセキュアメモリ305に格納する。

[0071] タイトルとは、情報処理装置(ユーザデバイス)400が装着した情報記録媒体200に格納したコンテンツに対応するタイトルである。

[0072] サービス提供状況データベースのデータ構成例を図8に示す。サービス提供状況データベースには、図8に示すように、サービス提供サーバ300が提供するサービス対応のコンテンツのタイトル識別情報、タイトル固有値毎に設定されており、そのタイトルのコンテンツを格納したディスクの各ディスクIDに対する各サービスの提供状況が格納される。

[0073] たとえば図8(a)に示すサービス提供状況データは、

タイトル識別情報:aaaa

タイトル固有値:bbbb

についてのサービス提供状況データであり、

このタイトル対応のコンテンツに対応するサービス1とサービス2について、ディスクID1とディスクID2のそれぞれのディスクに基づくサービス提供要求に対してこれまでに何度サービスを提供したかを記録している。

[0074] なお、図8(a)に示すサービス提供状況データにおいて、

サービス1は、ディスクID1つにつき1度まで提供可能なサービス

サービス2は、ディスクID1つにつき5回まで提供可能なサービス

であると規定されたサービスである。

[0075] サービス提供サーバ300は、図8に示すサービス提供状況データを、例えばセキュアメモリ305に格納し保持し、情報処理装置(ユーザデバイス)400からのディスクIDを伴うサービス提供要求に応じて、サービス提供要求デバイスが、正当なディスクIDに基づくサービス要求であるかの確認を実行し、さらに、図8に示すサービス提供状況データに基づいてサービス提供が許容上限に達していない場合に限り、サービスの提供を行なう。

[0076] サービス提供サーバ300は、情報処理装置(ユーザデバイス)400からのディスクIDを伴うサービス提供要求を受信すると、情報処理装置(ユーザデバイス)400から送信されるディスクIDの正当性の確認、サービス提供サーバ300の保有するリボケーションリストにおいて情報処理装置(ユーザデバイス)400から送信されるディスクIDがリボークされていないことの確認を行う。

[0077] さらに、正当性の確認されたディスクIDに基づくタイトル固有値の確認または取り出

し、ディスク固有値の取り出しなどの処理を実行する。サービス提供サーバ300は、取得したタイトル固有値に基づいて、図8に示すサービス提供状況データを格納したデータベースから、対応タイトルに対するサービス提供状況データを特定し、そのデータに基づいて、サービスを提供してよいかをチェックする。すなわち、図8に示すサービス提供状況データに基づいてサービス提供が許容上限に達していない場合に限り、サービスの提供を行なう。

[0078] なお、図8に示すサービス提供状況データの構成例では、ディスクID毎にサービス提供状況のデータを格納する例を示しているが、ディスクIDの代わりに、個々のディスクを識別するためのディスク固有値を使用する構成としてもよい。

[0079] なお、サービス提供サーバ300が情報処理装置(ユーザデバイス)400に対して、サービスの提供を実行した場合は、図8に示すサービス提供状況データを更新する処理を実行する。

[0080] 次に、図9を参照して、情報処理装置(ユーザデバイス)400の構成について説明する。

[0081] 図9に示すように、情報処理装置(ユーザデバイス)400は、例えば、入出力インタフェース402、MPEG(Moving Picture Experts Group)等の各種符号化データの生成および復号を実行するコーデック403、A/D・D/Aコンバータ405を備えた入出力インタフェース404、暗号処理部406、ROM(Read Only Memory)407、コントローラ408、メモリ409、並びに情報記録媒体200にアクセスするための記録媒体インタフェース410を有し、これらがバス401によって相互に接続されている。

[0082] 入出力インタフェース402は、ネットワーク等、外部から供給されるデジタル信号を受信し、バス401上に出力するとともに、バス401上のデジタル信号を受信し、外部に出力する。

[0083] コーデック403は、バス401を介して供給される例えばMPEG符号化されたデータをデコードし、入出力インタフェース404に出力するとともに、入出力インタフェース404から供給されるデジタル信号をエンコードしてバス401上に出力する。

[0084] 入出力インタフェース404は、A/D, D/Aコンバータ405を内蔵している。入出力インタフェース404は、外部から供給されるアナログ信号を受信し、A/D, D/A

コンバータ405でA／D（Analog Digital）変換することで、デジタル信号として、コーデック403に出力するとともに、コーデック403からのデジタル信号をA／D，D／Aコンバータ405でD／A（Digital Analog）変換することで、アナログ信号として、外部に出力する。

[0085] 暗号処理部406は、例えば、1チップのLSIで構成され、バス401を介して供給される例えばコンテンツ等のデジタル信号を暗号化し、または復号し、バス401上に出力する構成を持つ。なお、暗号処理部406は1チップLSIに限らず、各種のソフトウェアまたはハードウェアを組み合わせた構成によって実現することも可能である。

[0086] ROM407は、例えば、ユーザデバイスとしての情報処理装置ごとに固有の、あるいは複数の情報処理装置（ユーザデバイス）のグループごとに固有のデバイス鍵データであるリーフ鍵データと、複数の再生装置、あるいは複数のグループに共有のデバイス鍵データであるノード鍵データを記憶している。これらは、前述した暗号鍵情報としての有効化鍵ブロック（EKB）の復号処理に適用される。

[0087] コントローラ408は、例えばメモリ409に記憶されたプログラムを実行するCPUなどによって構成される。コントローラ408は、情報処理装置（ユーザデバイス）400の処理を統括して制御する。すなわち、情報処理装置（ユーザデバイス）400の機能（処理）は、コントローラ408の実行するプログラムによって規定される。

[0088] メモリ409は、上述したディスクIDリボケーションリスト（DIRL）を情報記録媒体200から読み取りセキュアな状態で格納する。例えば情報処理装置（ユーザデバイス）400に設定されたIDに基づく暗号化を施してメモリに格納するなどにより耐タンパ性を保持したデータとして格納することが好ましい。このようにディスクIDリボケーションリスト（DIRL）は外部から消されたり、内容を改ざんされたり、古いバージョンのリストに入れ替えられることを容易に実行されないように格納する。記録媒体インタフェース410は、情報記録媒体200にアクセスするために用いられる。

[0089] ［4．ユーザデバイスにおける処理の詳細］

次に、ユーザデバイスとしての情報処理装置400が、サービス提供サーバ300からサービスを受領する際の処理の詳細について説明する。

[0090] 図10は図9に示す情報処理装置（ユーザデバイス）400が、情報記録媒体を装着

し、サービス提供サーバからのサービスを受領する際に実行するシーケンスを説明するフローチャートである。

[0091] ステップS101において、情報処理装置(ユーザデバイス)400は、所定のアクセス位置に情報記録媒体200がセットされると、記録媒体インタフェース410を介して、情報記録媒体200からディスクIDを読み出し、これをメモリ409に格納する。

[0092] ステップS102において、情報処理装置(ユーザデバイス)400のコントローラ408は、メモリ409に格納したディスクIDを読み出してその改竄の有無および正当性を検証する。当該検証処理については、後に詳細に説明する。

[0093] ステップS103において、コントローラ408は、ステップS102で上記ディスクIDが正当であると判定するとステップS105の処理に進み、そうでない場合にはステップS104に進み、ステップS104において、コントローラ408は、情報記録媒体200に記録されている暗号化コンテンツの復号および再生を停止(禁止)する。

[0094] ディスクIDが正当であると判定した場合は、ステップS105において、コントローラ408は、記録媒体インタフェース410を介して、情報記録媒体200からディスクIDリボケーションリスト(DIRL)を読み出す。そして、コントローラ408は、当該読み出したリボケーションリストの改竄検証値として公開鍵暗号技術を用いたデジタル署名がなされている場合は、署名検証鍵(公開鍵)によって検証する。また、改竄検証値としてメッセージ認証コードMACが付与されている場合は、先に図3を参照して説明したMAC検証処理が実行される。

[0095] コントローラ408は、ディスクIDリボケーションリスト(DIRL)に改竄がないと判定されたことを条件に、当該ディスクIDリボケーションリスト(DIRL)のバージョンと、メモリ409に既に格納されているディスクIDリボケーションリスト(DIRL)とのバージョン比較を実行する。

[0096] コントローラ408は、読み出したディスクIDリボケーションリスト(DIRL)のバージョンがメモリ409に既に格納されているディスクIDリボケーションリスト(DIRL)より新しい場合は、読み出したディスクIDリボケーションリスト(DIRL)によって、メモリ409内のリボケーションリストDIRLを更新する。

[0097] ステップS106において、コントローラ408は、ステップS101で読み出したディスクI

Dがリボケーションリスト DIRL内に存在するか否かを判断し、存在すると判断するとステップS107に進み、そうでない場合にはステップS108に進む。ステップS107では、コントローラ408は、情報記録媒体200に記録されている暗号化コンテンツの復号および再生を停止(禁止)する。

[0098] ディスクIDがリボケーションリスト内に存在しなかった場合は、ステップS108に進み、コントローラ408は、ステップS101で読み出したディスクIDをサービス提供サーバに送信する。さらに、ステップS109において、サービス提供サーバからのサービスを受領する。なお、サービス提供サーバは、ステップS108において、情報処理装置(ユーザデバイス)400から受領したディスクIDの検証を実行して、正当性が確認された場合にのみ、サービスの提供処理を実行することになる。

[0099] 以下、ステップS102において実行するディスクIDの検証処理について説明する。情報記録媒体に格納されるディスクIDは、偽造困難性の高い識別情報として設定される。ディスクIDの構成例を図11に示す。

[0100] 図11には、情報記録媒体識別子としての情報記録媒体ID(ディスクID)と、情報記録媒体に格納したコンテンツのタイトルに対して設定される固有値であるタイトル固有値と、情報記録媒体の固有値として設定されるディスク固有値との対応例として6種類のディスクID設定例を示している。なお、ディスクID、ディスク固有値は、いずれも管理装置201が生成する。タイトル固有値:Mは、情報記録媒体に格納したコンテンツを構成する一部情報を適用してもよいし、あるいは管理装置201、コンテンツ提供装置203が生成する構成としてもよい。タイトル固有値:Sは、管理装置201がタイトル固有値:Mに基づいて生成する。

[0101] 図11に示す各記号の意味は、以下の通りである。

M:情報記録媒体の格納コンテンツのタイトルに対応する固有値

w:w=1, 2, ・・・Wであり、Wは、製造する情報記録媒体の枚数

Sig(w):管理装置の秘密鍵(例えば公開鍵暗号方式に基づいて設定された秘密鍵)に基づく署名データ、製造する情報記録媒体の枚数Wに応じて生成され、各情報記録媒体毎に異なる署名データとなる。Sig(w)は各ディスクの署名がSig(1), Sig(2)・・Sig(W)として設定されることを意味している

p(w):製造する情報記録媒体の枚数Wに対応して設定される素数、製造する情報記録媒体の枚数Wに応じて生成される各情報記録媒体毎に異なる素数データとなる

S:情報記録媒体の格納コンテンツのタイトルに対応する固有値であり、$S=K^{T} \bmod M$、ただし、Tは下記式によって算出される値

[数1]

$$T=\prod_{w=1}^{W} p_{w}$$

[0102] IDKey(w):$IDKey(w)=K^{T/p(w)} \bmod M$

ただし、Kは、各タイトルに対して設定される値であり、$K \in Z^{*}_{M}$(Kは巡回群Z^{*}_{M}の生成元、なお、$X \in Z^{*}_{M}$は、Xが1ーX−1の整数xの中でxを法として逆元を持つ集合要素であることを示す)を満たす値である

[0103] e(w):$e(w) \in Z^{*}_{M}$を満足するディスク製造枚数Wに対応する数の異なる値

ただし、e(w)とλ(M)は互いに素、すなわちe(w)とλ(M)の最大公約数が1である。なお、λ(M)は素数(q1−1)と(q2−1)の最小公倍数である。q1,q2は、RSA暗号に適用するのに必要とされる程度に大きな素数である。

[0104] I(w):$I(w)=S^{d(w)} \bmod M$

ただし、d(w)は、λ(M)を法としたときのe(w)の逆数である

Σw:データSと、データe(w)の連結データであるメッセージM(w)を管理装置(CA)201の秘密鍵で暗号化したデータ

[0105] 以下、図11に示す6つの異なるディスクIDの設定例に対応した情報処理装置(ユーザデバイス)400におけるディスクIDの検証処理シーケンスを説明する。

[0106] 設定例1における情報処理装置(ユーザデバイス)400におけるディスクIDの検証処理シーケンスについて、図12を参照して説明する。

設定例1は、

ディスクID＝M，Sig(w)

タイトル固有値＝M

ディスク固有値＝Sig(w)

とした設定例である。

[0107] 情報処理装置(ユーザデバイス)400のコントローラ408は、ステップS201において、ディスクID(w)内の署名データSIG(w)を取り出す。なお、ディスクIDは、ディスク製造枚数Wとしたとき、w＝1，2・・・Wによって示される個々のディスク(w)によって異なる値となるので、ディスクID(w)として標記する。

[0108] ステップS202において、コントローラ408は、メモリ409から読み出した管理装置12(管理局CA)の公開鍵および公開されたパラメータを基に、ステップS201で読み出した署名データSIG(w)からメッセージM(w)'を生成する。メッセージの標記もディスクID(w)の標記と同様であり、ディスク毎に異なるメッセージが対応付けられていることをM(w)で示している。

[0109] ステップS203において、コントローラ408は、ディスクID(w)内に含まれるメッセージM(w)と、ステップS202で生成したメッセージM(w)'とを比較する。

[0110] ステップS204において、コントローラ408は、ステップS203の比較処理で一致していると判定するとステップS205に進み、そうでない場合にはステップS206に進む。

[0111] ステップS205において、コントローラ408は、ステップS201で取り出したディスクID(w)が正当であると判定する。ステップS206では、コントローラ408は、ステップS201で取り出したディスクID(w)が不正であると判定する。

[0112] 設定例2は、

ディスクID＝S，Sig(w)

タイトル固有値＝S

ディスク固有値＝Sig(w)

とした設定例である。

この設定例2は、設定例1におけるタイトル固有値MをSに置き換えたのみであり、設定例1における情報処理装置(ユーザデバイス)400におけるディスクIDの検証処

理シーケンスと、同様のシーケンスであり、ステップS202において署名データから生成するデータがメッセージS'(w)となり、ステップS203における比較データがディスクIDに含まれるデータS(w)となる点が異なるのみである。

[0113] 次に、設定例3における情報処理装置(ユーザデバイス)400におけるディスクIDの検証処理シーケンスについて、図13を参照して説明する。

設定例3は、

ディスクID=p(w), IDKey(w)

タイトル固有値=S

ディスク固有値=p(w)またはIDKey(w)

とした設定例である。

[0114] ステップS301において、情報処理装置(ユーザデバイス)400のコントローラ408は、情報記録媒体200から読み出したディスクID(w)内のデータp(w)を取り出す。

[0115] ステップS302において、コントローラ408は、ステップS302で取り出したデータp(w)が素数であるか否かを判断する。コントローラ408は、データp(w)が素数であると判断するとステップS303に進み、そうでない場合にはステップS304に進む。

[0116] ステップS303で、コントローラ408は、ステップS301で取り出したディスクID(w)が正当であると判定する。ステップS304では、コントローラ408は、ステップS301で取り出したディスクID(w)が不正であると判定する。

[0117] 次に、設定例4における情報処理装置(ユーザデバイス)400におけるディスクIDの検証処理シーケンスについて、図14を参照して説明する。

設定例4は、

ディスクID=e(w), I(w)

タイトル固有値=S

ディスク固有値=e(w)またはI(w)

とした設定例である。

[0118] ステップS401において、情報処理装置(ユーザデバイス)400は、所定のアクセス位置に情報記録媒体200がセットされると、記録媒体インタフェース410を介して、情報記録媒体200からディスクIDを読み出し、これをメモリ409に格納する。

[0119] ステップS402において、情報処理装置(ユーザデバイス)400のコントローラ408は、メモリ409に記録したディスクID内のデータe(w)とI(w)とを用いて、$I(w)^{e(w)}$ modMを算出し、その結果をデータS'とする。すなわち、

$S' = I(w)^{e(w)} \mathrm{mod} M$

とする。

[0120] ステップS403において、コントローラ408は、記録媒体インタフェース410を介して、情報記録媒体200からディスクIDリボケーションリスト(DIRL)を読み出す。コントローラ408は、読み出したディスクIDリボケーションリスト(DIRL)の改竄検証値として公開鍵暗号技術を用いたデジタル署名がなされている場合は、署名検証鍵(公開鍵)によって検証する。また、改竄検証値としてメッセージ認証コードMACが付与されている場合は、先に図3を参照して説明したMAC検証処理が実行される。

[0121] コントローラ408は、ディスクIDリボケーションリスト(DIRL)に改竄がないと判定されたことを条件に、当該ディスクIDリボケーションリスト(DIRL)のバージョンと、メモリ409に既に格納されているディスクIDリボケーションリスト(DIRL)とのバージョン比較を実行する。コントローラ408は、当該読み出したディスクIDリボケーションリスト(DIRL)のバージョンがメモリ409に既に格納されているディスクIDリボケーションリスト(DIRL)より新しい場合は、読み出したディスクIDリボケーションリスト(DIRL)によって、メモリ409内のリボケーションリストDIRLを更新する。

[0122] ステップS404において、コントローラ408は、ステップS401で読み出したディスクIDがリボケーションリスト内に存在するか否かを判断し、存在すると判断するとステップS405に進み、そうでない場合にはステップS406に進む。

[0123] ステップS405では、コントローラ408は、情報記録媒体200cに記録されているコンテンツの再生を停止(禁止)する。ステップS406では、コントローラ408は、ステップS401で読み出したディスクIDをサービス提供サーバに送信する。さらに、ステップS407において、サービス提供サーバからのサービスを受領する。なお、サービス提供サーバは、ステップS406において、情報処理装置(ユーザデバイス)400から受領したディスクIDの検証を実行して、正当性が確認された場合にのみ、サービスの提供処理を実行することになる。

[0124] 次に、設定例5における情報処理装置（ユーザデバイス）400におけるディスクIDの検証処理シーケンスについて、図15を参照して説明する。

設定例5は、

ディスクID＝Σw

タイトル固有値＝S

ディスク固有値＝e（w）

とした設定例である。

[0125] ステップS501において、情報処理装置（ユーザデバイス）400のコントローラ408は、情報記録媒体200から読み出したディスクID（w）を、管理装置201（管理局CA）の公開鍵データを基に復号してメッセージM（w）を生成する。メッセージM（w）は、前述したように、データSと、データe（w）とが連結されたデータである。

[0126] ステップS502において、情報処理装置（ユーザデバイス）400は、管理装置201によって公開されたサイズ｜S｜、並びにサイズ｜e（w）｜、並びにデータSとデータe（w）との組み合わせパターンとを基に、ステップS501で復号されたメッセージM（w）から、データSを取り出す。

[0127] 情報処理装置（ユーザデバイス）400は、上述した図15に示す処理に続いて、図10に示すステップS105ーS109の処理を行う。この場合に、情報処理装置（ユーザデバイス）400は、図10に示すステップS105，S106におけるリボケーションリストとのディスクID照合処理において、ディスクIDとしてステップS501で情報記録媒体200から読み出したディスクID（w）を用いる。

[0128] 情報処理装置（ユーザデバイス）400は、ステップS502で取り出したデータSをコンテンツ鍵データとして用いて、コンテンツデータを復号する。従って、上記ステップS501，S502の処理を経て適切なデータSを取得できない場合には、コンテンツデータを適切に復号できない。

[0129] 設定例6は、

ディスクID＝p（w），IDKey（w）

タイトル固有値＝S

ディスク固有値＝p(w)

とした設定例であり、これは設定例3とディスクIDの構成が同様であるので、先に図13を参照して説明した処理と同様のディスクID検証処理が実行されることになる。

[0130] ［5．サービス提供サーバにおける処理の詳細］

次に、サービス提供サーバ300が、情報処理装置(ユーザデバイス)400からのサービス提供要求を受信した際の処理について説明する。

[0131] 図16に示すように、サービス提供サーバ300は、情報処理装置(ユーザデバイス)400から、ディスクIDを受信する。このディスクIDは、情報記録媒体200を装着し、情報記録媒体200からのディスクIDの読み取り処理を実行した情報処理装置(ユーザデバイス)400において検証処理によって正当性を検証したディスクIDである。

[0132] サービス提供サーバ300は、情報処理装置(ユーザデバイス)400からサービス提供要求に併せてディスクIDを受信すると、ディスクIDの正当性を検証して、正当性の確認されたことを条件としてサービスを提供する。

[0133] なお、情報処理装置(ユーザデバイス)400からサービス提供要求に併せてディスクIDとともにサービス識別子としてのサービスIDもサービス提供サーバ300に送信する。

[0134] サービス提供サーバ300は、図7に示す入出力インタフェース(I／F)304を介して、管理装置201またはコンテンツ提供装置203またはその他の装置からディスクIDリボケーションリストを定期的に、またはイベントごとに受信し、常に最新版をセキュアメモリ305に格納する処理を実行し、また、入出力インタフェース(I／F)304を介して、コンテンツ提供装置203またはその他の装置から、タイトルごとのタイトル固有値と、提供するサービスを識別するサービス識別情報を受信し、先に図8を参照して説明したタイトルごとのサービス提供状況情報を管理したサービス提供状況データベースをセキュアメモリ305に格納している。

[0135] サービス提供サーバ300は、図8に示すサービス提供状況データを、例えばセキュアメモリ305に格納し保持し、情報処理装置(ユーザデバイス)400からのディスクIDを伴うサービス提供要求に応じて、サービス提供要求デバイスが、正当なディスクIDに基づくサービス要求であるかの確認を実行し、さらに、図8に示すサービス提供状

況データに基づいてサービス提供が許容上限に達していない場合に限り、サービスの提供を行なう。

[0136] 図17を参照して、サービス提供サーバ300が、情報処理装置(ユーザデバイス)400からのサービス提供要求を受信した際の処理シーケンスについて説明する。

[0137] ステップS701において、サービス提供サーバ300は、図7に示す入出力インタフェース(I/F)304を介して、情報処理装置(ユーザデバイス)400からのサービス提供要求を受信する。この情報処理装置(ユーザデバイス)400からのサービス提供要求には情報処理装置(ユーザデバイス)400が、情報記録媒体200から取得したディスクIDと、要求サービスの識別子(サービス識別子)が含まれる。ディスクIDは、先に図11を参照して説明した設定例1ー6のいずれかのディスクIDである。

[0138] ステップS702において、サービス提供サーバ300は、受信したディスクIDの検証処理を実行する。この検証処理は、情報処理装置(ユーザデバイス)400において実行する検証処理と同様の検証シーケンス、すなわち、図12ー図15を参照して説明したディスクIDの設定例1ー6に応じた検証シーケンスを実行する。

[0139] ステップS703において、ディスクIDの検証処理によってディスクIDの正当性が確認されると、ステップS705に進み、ディスクIDが不正であると判定されると、ステップS704に進みサービスの提供処理を中止する。なお、この中止処理の際に、情報処理装置(ユーザデバイス)400に対するサービス提供処理の中止メッセージを送信する処理を行なう構成としてもよい。

[0140] ディスクIDの正当性が確認され、ステップS705に進んだ場合は、セキュアメモリ305(図7参照)に格納されたディスクIDリボケーションリスト(DIRL)を読み出す。

[0141] ステップS706において、正当性確認の済んだ受信ディスクIDがリボケーションリストに記録されていないかを判定する。

[0142] 受信ディスクIDがリボケーションリストに記録されている場合は、不正IDであると判定し、ステップS711に進み、サービスの提供処理を中止する。なお、この中止処理の際に、情報処理装置(ユーザデバイス)400に対するサービス提供処理の中止メッセージを送信する処理を行なう構成としてもよい。

[0143] 受信ディスクIDがリボケーションリストに記録されていない場合は、ステップS707に

おいて、ディスクIDに基づいてタイトル固有値を算出する。ディスクIDは先に図11を参照して説明したタイトル固有値MまたはSを含むデータ、あるいはタイトル固有値MまたはSを算出可能なデータとして構成されており、サービス提供サーバ300は、受信したディスクIDに含まれるタイトル固有値MまたはSを取得、あるいは、演算ユニット303の演算処理により、受信したディスクIDからタイトル固有値MまたはSを算出する。このタイトル固有値MまたはSの取得、算出処理は、先に図11を参照して説明した設定例1ー6に応じて異なる処理として実行されることになる。

[0144] ステップS707では、さらに、ディスクIDから取得したタイトル固有値MまたはSに基づいて、タイトル対応のサービス提供状況データをデータベースから取得する。すなわち、図8を参照して説明したサービス提供状況データであり、各ディスクIDに対応する各サービスの提供状況を設定したデータである。

[0145] ステップS707において、サービス提供状況データ中から、情報処理装置(ユーザデバイス)400から受信したディスクIDとサービス識別子に対応するデータを抽出し、提供可能なサービスであるか否かをチェックする。

[0146] 図8に示すサービス提供状況データを例にして説明すると、例えば、情報処理装置(ユーザデバイス)400から受信したディスクIDが(DiscID1)であり、サービス識別子が(サービス1)である場合、サービス1は上限1回であり、サービス提供状況は、[未提供]であるので、提供可能と判断される。

[0147] ステップS708において、サービス提供状況データに基づいてサービス提供可能と判定すると、ステップS709に進み、ステップS708において、サービス提供状況データに基づいてサービス提供不可能と判定すると、ステップS711に進む。

[0148] ステップS711では、サービスの提供処理を中止する。なお、この中止処理の際に、情報処理装置(ユーザデバイス)400に対するサービス提供処理の中止メッセージを送信する処理を行なう構成としてもよい。

[0149] サービス提供状況データに基づいてサービス提供可能と判定した場合は、ステップS709において、データベースの更新を行なう。

[0150] 図8に示すサービス提供状況データを例にして説明すると、例えば、情報処理装置(ユーザデバイス)400から受信したディスクIDが(DiscID1)であり、サービス識別子

が（サービス1）である場合、サービス提供状況は、［未提供］を［提供1回済］に変更する。

[0151] ステップS710では、サービス提供サーバ300は、サービス提供要求を送信してきた情報処理装置（ユーザデバイス）400に対するサービス提供処理を実行する。

[0152] 例えば、ディスク格納コンテンツが外国語映画である場合の音声に対する字幕データや吹き替え音声データ、あるいはコンテンツの続編のディスクの購入割引券など、様々なコンテンツ関連サービスが、ネットワークを介してサービス提供サーバ300から情報処理装置（ユーザデバイス）400に提供される。

[0153] なお、情報処理装置（ユーザデバイス）400とサービス提供サーバ300間の通信は、暗号技術を用いた相互認証、およびセッションキーの共有を行って安全な通信路を作成し、その上で通信を行うことが望ましい。

[0154] また、上述の例では、サービス提供要求を受領するたびにステップS705、S706においてディスクIDリボケーションリスト（DIRL）をチェックするようになっているが、あらかじめ、たとえば定期的にディスクIDリボケーションリスト（DIRL）をチェックし、そこにリストされたディスクIDについてはデータベースを更新してそれ以上のサービス提供を行わないようにしておく構成としてもよい。このような構成とした場合には、サービス提供要求を受領した際のディスクIDリボケーションリスト（DIRL）のチェックを省くことができ、サービスを提供するための時間を短くすることもできる。

[0155] また、上述した実施例ではディスクIDはディスク1枚ごとに異なるものとして説明してきたが、ディスクIDをたとえば10枚、100枚、1000枚といったグループ単位で共通とし、ディスクIDひとつに対して提供するサービスの回数をグループの枚数を考慮して決定してもよい。

[0156] 以上、特定の実施例を参照しながら、本発明について詳解してきた。しかしながら、本発明の要旨を逸脱しない範囲で当業者が該実施例の修正や代用を成し得ることは自明である。すなわち、例示という形態で本発明を開示してきたのであり、限定的に解釈されるべきではない。本発明の要旨を判断するためには、冒頭に記載した特許請求の範囲の欄を参酌すべきである。

[0157] なお、明細書中において説明した一連の処理はハードウェア、またはソフトウェア、

あるいは両者の複合構成によって実行することが可能である。ソフトウェアによる処理を実行する場合は、処理シーケンスを記録したプログラムを、専用のハードウェアに組み込まれたコンピュータ内のメモリにインストールして実行させるか、あるいは、各種処理が実行可能な汎用コンピュータにプログラムをインストールして実行させることが可能である。

[0158] 例えば、プログラムは記録媒体としてのハードディスクやROM(Read Only Memory)に予め記録しておくことができる。あるいは、プログラムはフレキシブルディスク、CD−ROM(Compact Disc Read Only Memory), MO(Magneto optical)ディスク, DVD(Digital Versatile Disc)、磁気ディスク、半導体メモリなどのリムーバブル記録媒体に、一時的あるいは永続的に格納(記録)しておくことができる。このようなリムーバブル記録媒体は、いわゆるパッケージソフトウエアとして提供することができる。

[0159] なお、プログラムは、上述したようなリムーバブル記録媒体からコンピュータにインストールする他、ダウンロードサイトから、コンピュータに無線転送したり、LAN(Local Area Network)、インターネットといったネットワークを介して、コンピュータに有線で転送し、コンピュータでは、そのようにして転送されてくるプログラムを受信し、内蔵するハードディスク等の記録媒体にインストールすることができる。

[0160] なお、明細書に記載された各種の処理は、記載に従って時系列に実行されるのみならず、処理を実行する装置の処理能力あるいは必要に応じて並列的にあるいは個別に実行されてもよい。また、本明細書においてシステムとは、複数の装置の論理的集合構成であり、各構成の装置が同一筐体内にあるものには限らない。

産業上の利用可能性

[0161] 以上、説明したように、本発明の構成によれば、DVD、CD、青色レーザ記録媒体等の各種情報記録媒体にコンテンツを格納して提供し、さらにネットワーク接続したサービス提供サーバからのサービス提供処理を行なう構成において、サービス提供サーバ側において、情報処理装置(ユーザデバイス)から送信される情報記録媒体IDを検証し、情報記録媒体ID毎のサービス提供状況データに基づくサービス提供を行なう構成としたので、サービス要求を送信した情報処理装置が正当な情報記録媒体IDを情報記録媒体から読み取った情報処理装置であり、サービス提供状況デー

タに基づいてサービス提供が許容されているサービスであることが確認された場合に限り、サービスの提供が実行される。本発明の構成は、コンテンツに対応する様々なサービス情報、例えばディスク格納コンテンツが映画コンテンツである場合の字幕データ、吹き替え音声データなどのコンテンツに付随する情報をサーバから提供するシステムなどにおいて、サービス提供先を厳格に審査して、正当な権限を確認した上でコンテンツに対応する様々なサービス情報を提供することが可能となる。

[0162] さらに、本発明の構成によれば、情報記録媒体に格納された情報記録媒体IDは、管理装置の署名データなどの正当性の確認可能なデータを含み、また、タイトル固有値を有するかあるいは算出可能なデータを含む構成としたので、サービス提供サーバにおいては、情報記録媒体IDに含まれるデータに基づく正当性の確認が可能であり、また、タイトル固有値を取得することが可能となり、タイトル固有値に対応付けて設定されたサービス提供状況データの特定を行なうことが可能となる。従って、サービス提供先を厳格に審査して、正当な権限を確認した上でコンテンツに対応する様々なサービス情報を提供することが可能となる。

請求の範囲

[1] 情報処理装置からのサービス提供要求に応じたサービス提供処理を実行するサービス提供サーバであり、

情報処理装置からの情報記録媒体IDおよびサービスIDを伴うサービス要求を受信するデータ受信部と、

情報記録媒体の格納コンテンツのタイトルに対応するタイトル固有値毎のサービス管理データとして前記情報記録媒体ID毎のサービス提供状況データを格納した記憶部と、

前記データ受信部を介して受信した情報記録媒体IDの検証処理を実行し、正当性が確認されたことを条件として、該情報記録媒体IDに基づいてタイトル固有値を取得し、タイトル固有値に対応するサービス提供状況データを前記記憶部から取得して、前記情報記録媒体IDおよび前記サービスIDによって特定されるサービスの提供可否を判定し、提供可能であるとの判定を条件としたサービス提供処理を実行するデータ処理部と、

を有することを特徴とするサービス提供サーバ。

[2] 前記データ処理部は、

情報記録媒体IDの検証処理を情報記録媒体IDに含まれる署名データの検証処理として実行し、情報記録媒体IDに含まれるタイトル固有値、または情報記録媒体IDに含まれるデータに基づく演算を実行して算出したタイトル固有値に従って、タイトル固有値対応のサービス提供状況データを前記記憶部から取得する処理を実行する構成であることを特徴とする請求項1に記載のサービス提供サーバ。

[3] 前記サービス提供サーバは、不正な情報記録媒体IDのリストであるリボケーションリストを格納した記憶部を有し、

前記データ処理部における情報記録媒体IDの検証処理は、

情報処理装置から受信した情報記録媒体IDと、前記リボケーションリストに記録されたIDとの照合処理として実行することを特徴とする請求項1に記載のサービス提供サーバ。

[4] 前記情報記録媒体IDは、

情報記録媒体の格納コンテンツのタイトルに対応するタイトル固有値と、管理装置の秘密鍵に基づいて生成された情報記録媒体毎に異なる署名データとを含み、

前記データ処理部は、

前記情報記録媒体IDの検証処理を、前記情報記録媒体IDに含まれる署名データに対する前記管理装置の公開鍵を適用したメッセージ生成および照合処理として実行するとともに、情報記録媒体IDに含まれるタイトル固有値に対応するサービス提供状況データを前記記憶部から取得する処理を実行する構成であることを特徴とする請求項1に記載のサービス提供サーバ。

[5] 前記情報記録媒体IDは、

製造された情報記録媒体の枚数Wに対応して設定される素数p(w)と、

素数p(w)と、タイトル固有値に基づく演算によって算出されるデータIDKey(w)とを含み、

前記データ処理部は、前記情報記録媒体IDに含まれるデータが素数であるか否かを判定する処理をID検証処理として実行するとともに、情報記録媒体IDに含まれるデータIDKey(w)からタイトル固有値を算出し、算出したタイトル固有値に対応するサービス提供状況データを前記記憶部から取得する処理を実行する構成であることを特徴とする請求項1に記載のサービス提供サーバ。

[6] サービス提供サーバに対するサービス提供要求を実行する情報処理装置であり、

情報記録媒体のアクセス処理を実行する記録媒体インタフェースと、

前記記録媒体インタフェースを介して情報記録媒体から読み取られた情報記録媒体IDの検証処理を実行し、正当性が確認されたことを条件として、該情報記録媒体IDのサービス提供サーバに対する送信処理を実行するデータ処理部と、

を有することを特徴とする情報処理装置。

[7] 前記データ処理部は、

情報記録媒体IDの検証処理を、情報記録媒体IDに含まれる署名データの検証処理として実行する構成であることを特徴とする請求項6に記載の情報処理装置。

[8] 前記データ処理部における情報記録媒体IDの検証処理は、

不正な情報記録媒体IDのリストであるリボケーションリストを記憶部または情報記録

媒体から取得し、取得したリボケーションリストに記録されたIDと、情報処理装置から受信した情報記録媒体IDとの照合処理として実行する構成であることを特徴とする請求項6に記載の情報処理装置。

[9] 前記情報記録媒体IDは、

情報記録媒体の格納コンテンツのタイトルに対応するタイトル固有値と、管理装置の秘密鍵に基づいて生成された情報記録媒体毎に異なる署名データとを含み、

前記データ処理部は、

前記情報記録媒体IDの検証処理を、前記情報記録媒体IDに含まれる署名データに対する前記管理装置の公開鍵を適用したメッセージ生成および照合処理として実行する構成であることを特徴とする請求項6に記載の情報処理装置。

[10] 前記情報記録媒体IDは、

製造された情報記録媒体の枚数Wに対応して設定される素数p(w)と、

素数p(w)と、タイトル固有値に基づく演算によって算出されるデータIDKey(w)とを含み、

前記データ処理部は、

前記情報記録媒体IDに含まれるデータが素数であるか否かを判定する処理をID検証処理として実行する構成であることを特徴とする請求項6に記載の情報処理装置。

[11] 情報処理装置からのサービス提供要求に応じた処理を実行するデータ処理方法であり、

情報処理装置からの情報記録媒体IDおよびサービスIDを伴うサービス要求を受信するデータ受信ステップと、

受信した情報記録媒体IDの検証処理を実行し、正当性が確認されたことを条件として、該情報記録媒体IDに基づいてタイトル固有値を取得し、情報記録媒体の格納コンテンツのタイトルに対応するタイトル固有値毎のサービス管理データとして前記情報記録媒体ID毎のサービス提供状況データを格納した記憶部から、取得したタイトル固有値に対応するサービス提供状況データを取得して、前記情報記録媒体IDおよび前記サービスIDによって特定されるサービスの提供可否を判定し、提供可能で

あるとの判定を条件としたサービス提供処理を実行するデータ処理ステップと、

を有することを特徴とするデータ処理方法。

[12] 前記データ処理ステップは、

情報記録媒体IDの検証処理を情報記録媒体IDに含まれる署名データの検証処理として実行し、情報記録媒体IDに含まれるタイトル固有値、または情報記録媒体IDに含まれるデータに基づく演算を実行して算出したタイトル固有値に従って、タイトル固有値対応のサービス提供状況データを前記記憶部から取得する処理を実行するステップを含むことを特徴とする請求項11に記載のデータ処理方法。

[13] 前記データ処理ステップにおける情報記録媒体IDの検証処理は、

情報処理装置から受信した情報記録媒体IDと、不正な情報記録媒体IDのリストであるリボケーションリストに記録されたIDとの照合処理として実行するステップを含むことを特徴とする請求項11に記載のデータ処理方法。

[14] 前記情報記録媒体IDは、

情報記録媒体の格納コンテンツのタイトルに対応するタイトル固有値と、管理装置の秘密鍵に基づいて生成された情報記録媒体毎に異なる署名データとを含み、

前記データ処理ステップは、

前記情報記録媒体IDの検証処理を、前記情報記録媒体IDに含まれる署名データに対する前記管理装置の公開鍵を適用したメッセージ生成および照合処理として実行するとともに、情報記録媒体IDに含まれるタイトル固有値に対応するサービス提供状況データを前記記憶部から取得する処理を実行するステップを含むことを特徴とする請求項11に記載のデータ処理方法。

[15] 前記情報記録媒体IDは、

製造された情報記録媒体の枚数Wに対応して設定される素数p(w)と、

素数p(w)と、タイトル固有値に基づく演算によって算出されるデータIDKey(w)とを含み、

前記データ処理ステップは、

前記情報記録媒体IDに含まれるデータが素数であるか否かを判定する処理をID検証処理として実行するとともに、情報記録媒体IDに含まれるデータIDKey(w)か

らタイトル固有値を算出し、算出したタイトル固有値に対応するサービス提供状況データを前記記憶部から取得する処理を実行するステップを含むことを特徴とする請求項11に記載のデータ処理方法。

[16] サービス提供サーバに対するサービス提供要求を実行するデータ処理方法であり、

記録媒体インタフェースを介して情報記録媒体のアクセス処理を実行する情報記録媒体アクセスステップと、

前記記録媒体インタフェースを介して情報記録媒体から読み取られた情報記録媒体IDの検証処理を実行し、正当性が確認されたことを条件として、該情報記録媒体IDのサービス提供サーバに対する送信処理を実行するデータ処理ステップと、

を有することを特徴とするデータ処理方法。

[17] 前記データ処理ステップは、

情報記録媒体IDの検証処理を、情報記録媒体IDに含まれる署名データの検証処理として実行することを特徴とする請求項16に記載のデータ処理方法。

[18] 前記データ処理ステップにおける情報記録媒体IDの検証処理は、

不正な情報記録媒体IDのリストであるリボケーションリストを記憶部または情報記録媒体から取得し、取得したリボケーションリストに記録されたIDと、情報処理装置から受信した情報記録媒体IDとの照合処理として実行するステップを含むことを特徴とする請求項16に記載のデータ処理方法。

[19] 前記情報記録媒体IDは、

情報記録媒体の格納コンテンツのタイトルに対応するタイトル固有値と、管理装置の秘密鍵に基づいて生成された情報記録媒体毎に異なる署名データとを含み、

前記データ処理ステップは、

前記情報記録媒体IDの検証処理を、前記情報記録媒体IDに含まれる署名データに対する前記管理装置の公開鍵を適用したメッセージ生成および照合処理として実行するステップを含むことを特徴とする請求項16に記載のデータ処理方法。

[20] 前記情報記録媒体IDは、

製造された情報記録媒体の枚数Wに対応して設定される素数p(w)と、

素数p(w)と、タイトル固有値に基づく演算によって算出されるデータIDKey(w)とを含み、

前記データ処理ステップは、

前記情報記録媒体IDに含まれるデータが素数であるか否かを判定する処理をID検証処理として実行するステップを含むことを特徴とする請求項16に記載のデータ処理方法。

[21] 情報処理装置からのサービス提供要求に応じた処理を実行するコンピュータ・プログラムであり、

情報処理装置からの情報記録媒体IDおよびサービスIDを伴うサービス要求を受信するデータ受信ステップと、

受信した情報記録媒体IDの検証処理を実行し、正当性が確認されたことを条件として、該情報記録媒体IDに基づいてタイトル固有値を取得し、情報記録媒体の格納コンテンツのタイトルに対応するタイトル固有値毎のサービス管理データとして前記情報記録媒体ID毎のサービス提供状況データを格納した記憶部から、取得したタイトル固有値に対応するサービス提供状況データを取得して、前記情報記録媒体IDおよび前記サービスIDによって特定されるサービスの提供可否を判定し、提供可能であるとの判定を条件としたサービス提供処理を実行するデータ処理ステップと、

を有することを特徴とするコンピュータ・プログラム。

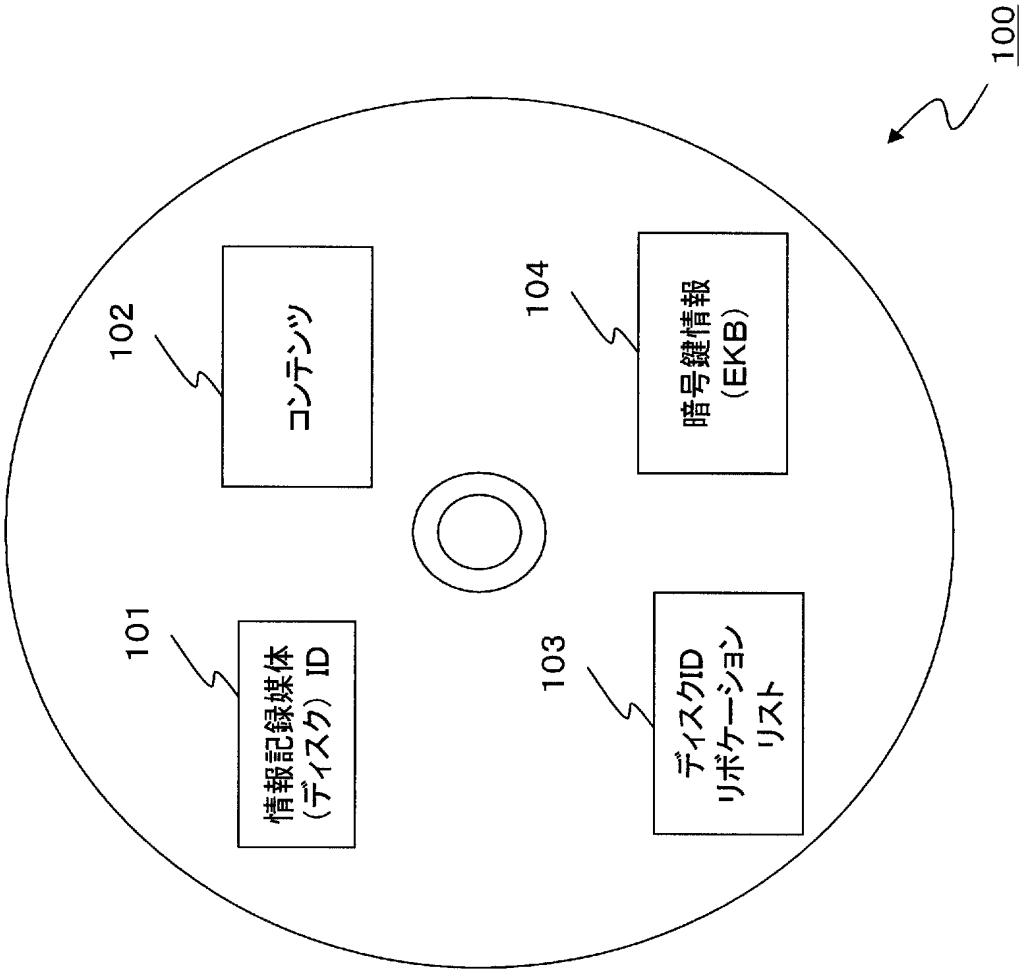
[22] サービス提供サーバに対するサービス提供要求を実行するコンピュータ・プログラムであり、

記録媒体インタフェースを介して情報記録媒体のアクセス処理を実行する情報記録媒体アクセスステップと、

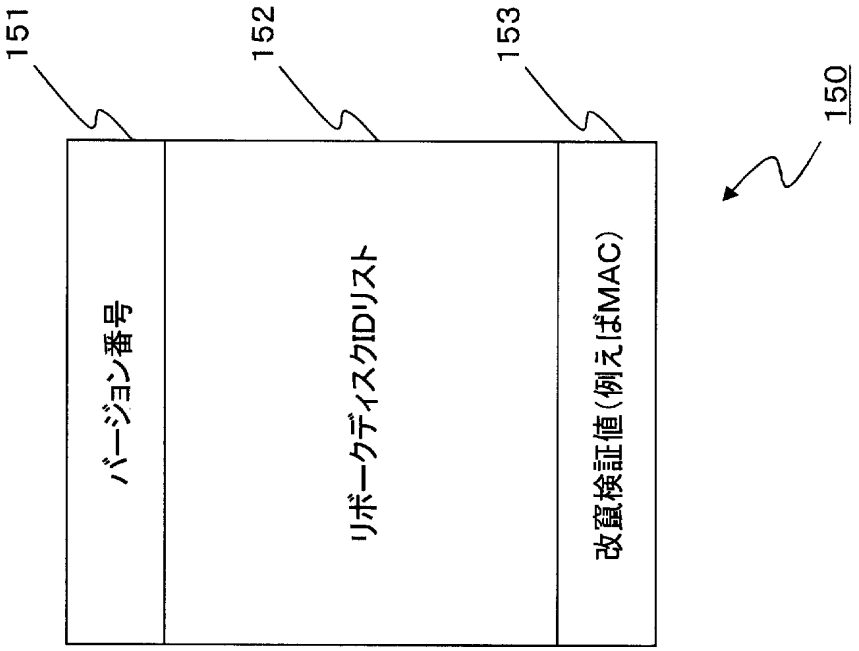
前記記録媒体インタフェースを介して情報記録媒体から読み取られた情報記録媒体IDの検証処理を実行し、正当性が確認されたことを条件として、該情報記録媒体IDのサービス提供サーバに対する送信処理を実行するデータ処理ステップと、

を有することを特徴とするコンピュータ・プログラム。

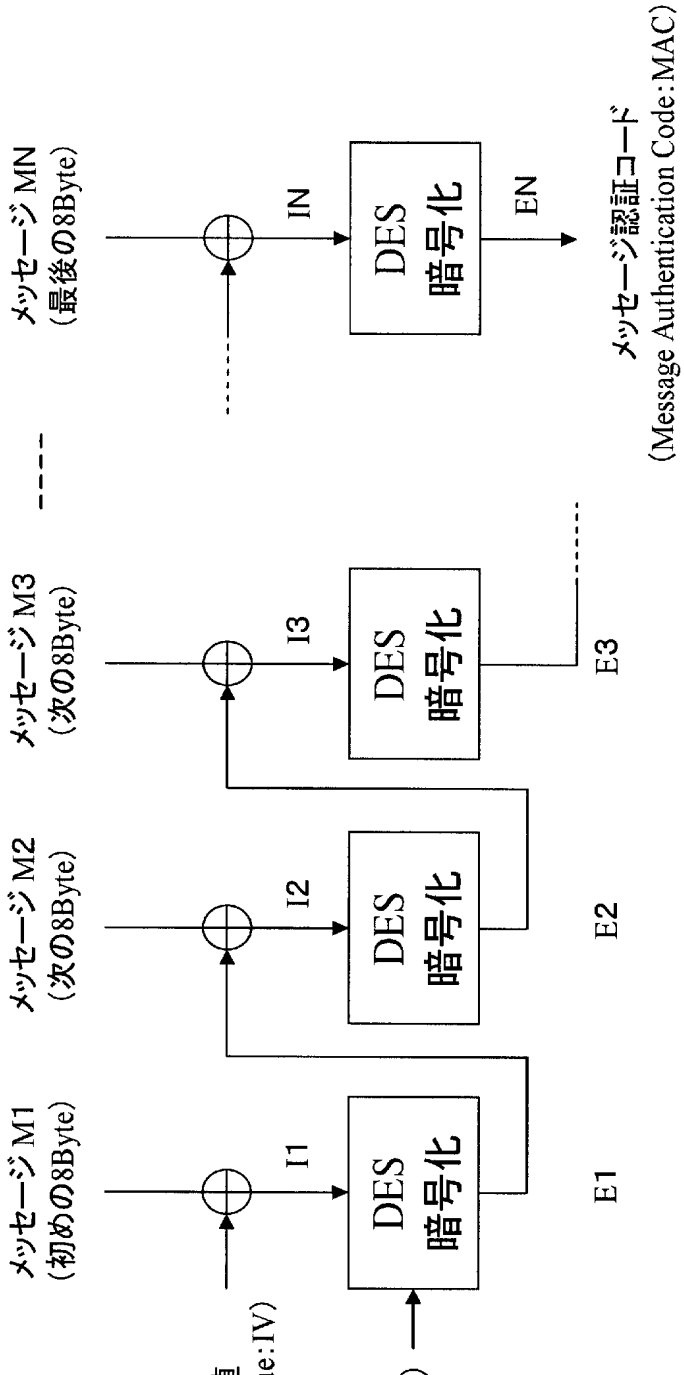
[図1]


100
101
情報記録媒体（ディスク）ID
102
コンテンツ
103
ディスクID リボケーション リスト
104
暗号鍵情報（EKB）

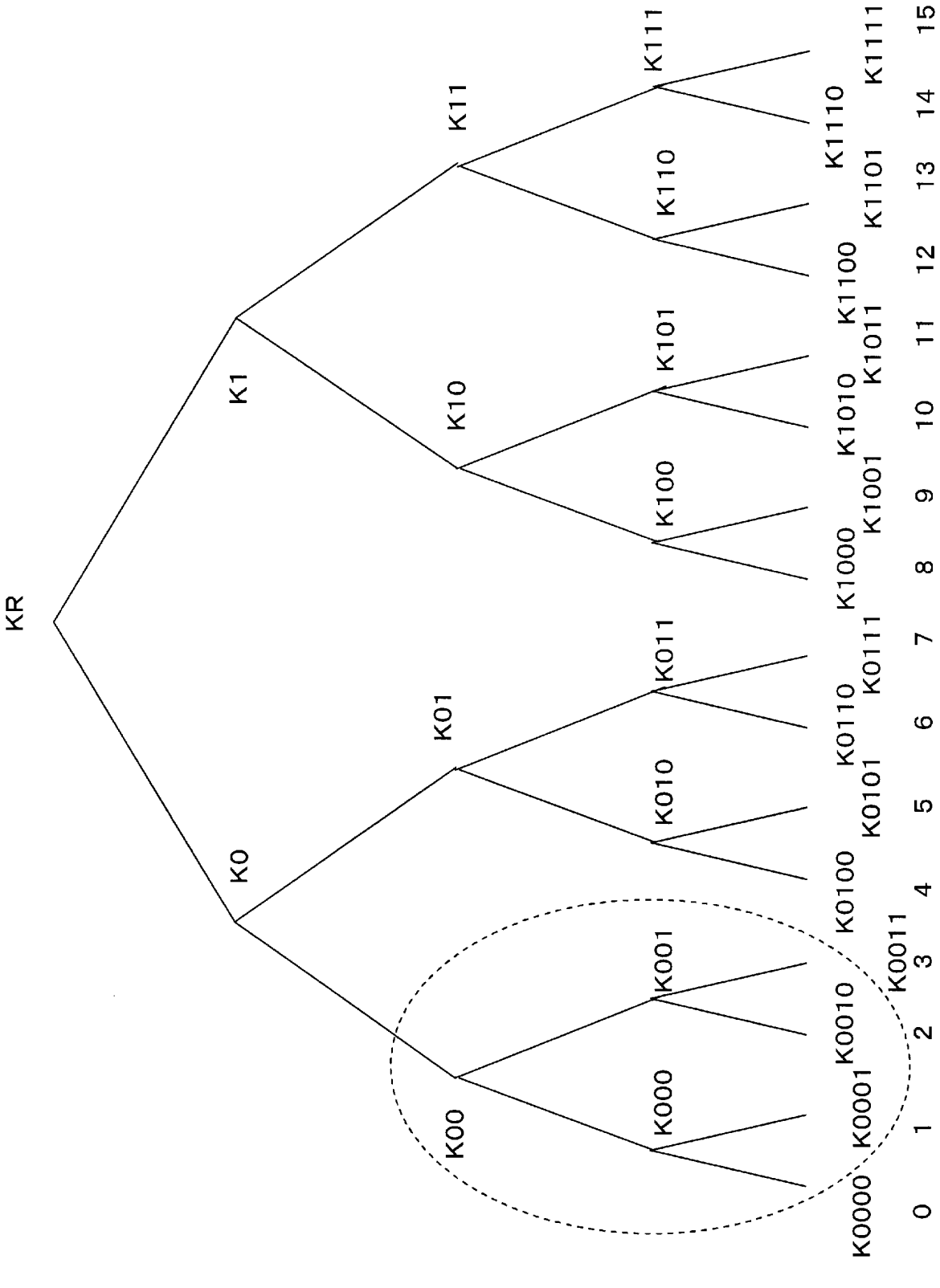
[図2]



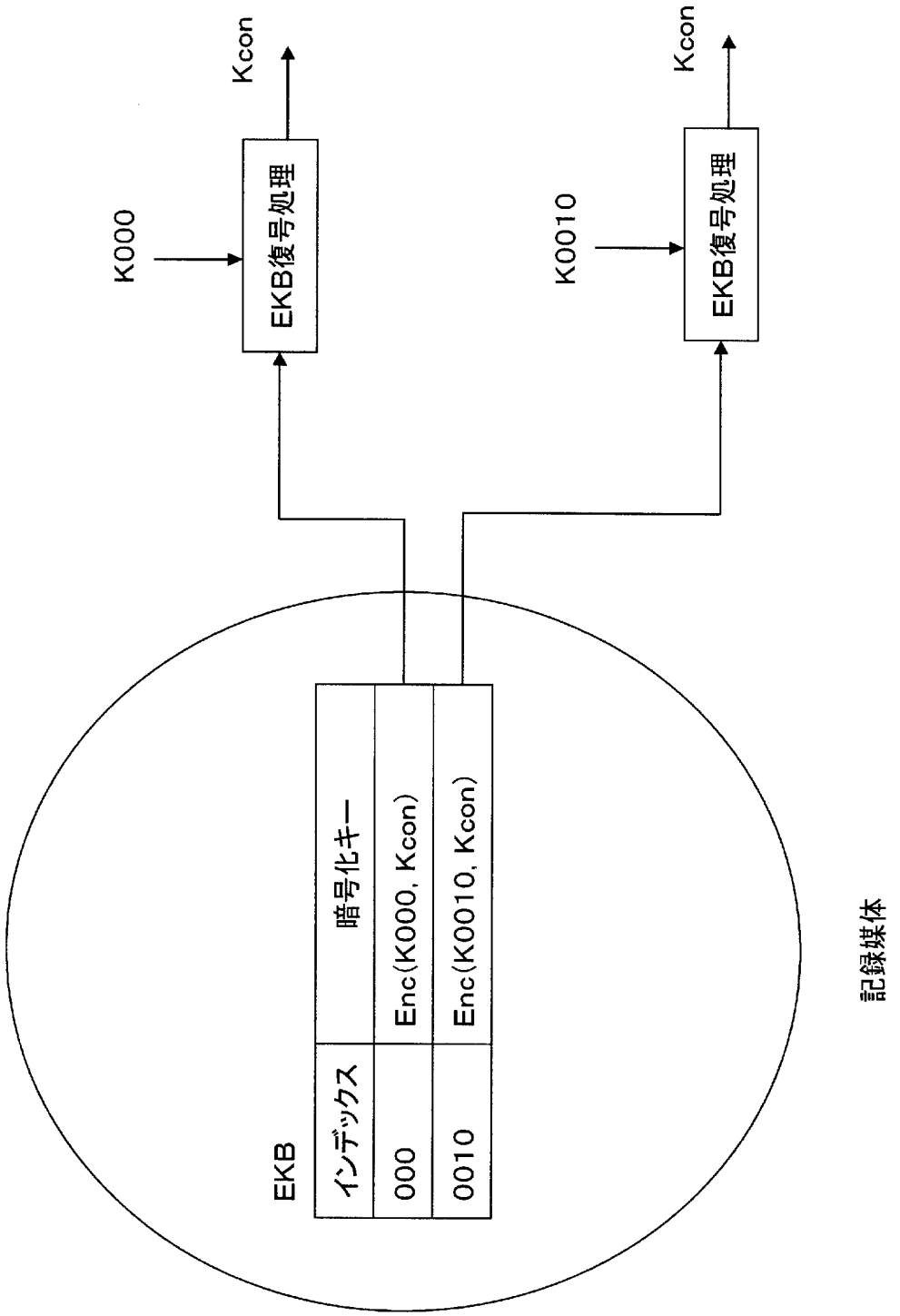
[図3]


メッセージ M1
(初めの8Byte)
メッセージ M2
(次の8Byte)
メッセージ M3
(次の8Byte)
メッセージ MN
(最後の8Byte)
初期値
(Initial Value:IV)
鍵(K1)
I1
I2
I3
IN
DES
暗号化
E1
E2
E3
EN
メッセージ認証コード
(Message Authentication Code:MAC)
:排他的論理和処理(8バイト単位)

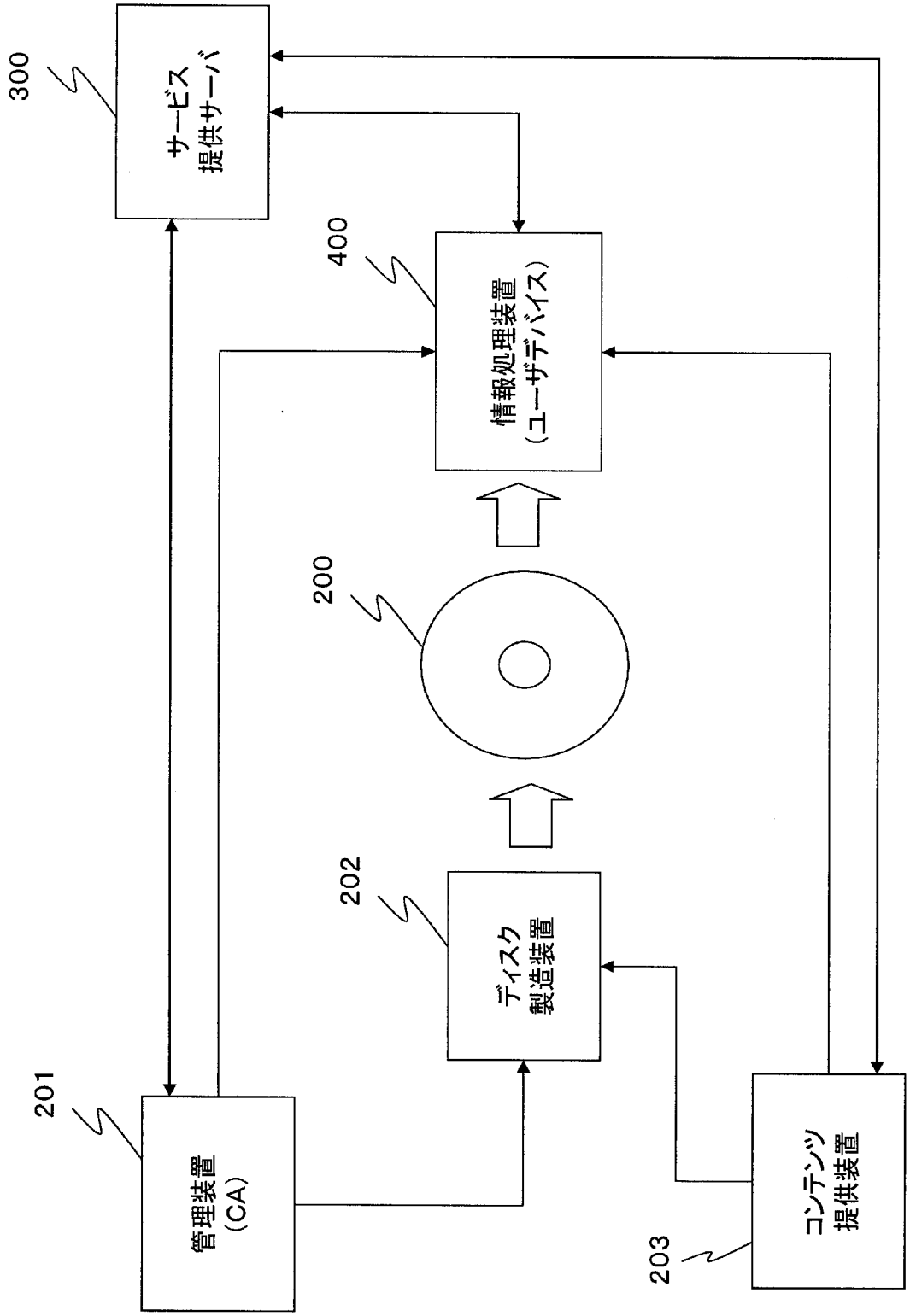
[図4]


KR
K0
K1
K00
K01
K10
K11
K000
K001
K010
K011
K100
K101
K110
K111
K0000
K0001
K0010
K0011
K0100
K0101
K0110
K0111
K1000
K1001
K1010
K1011
K1100
K1101
K1110
K1111
0
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
デバイス

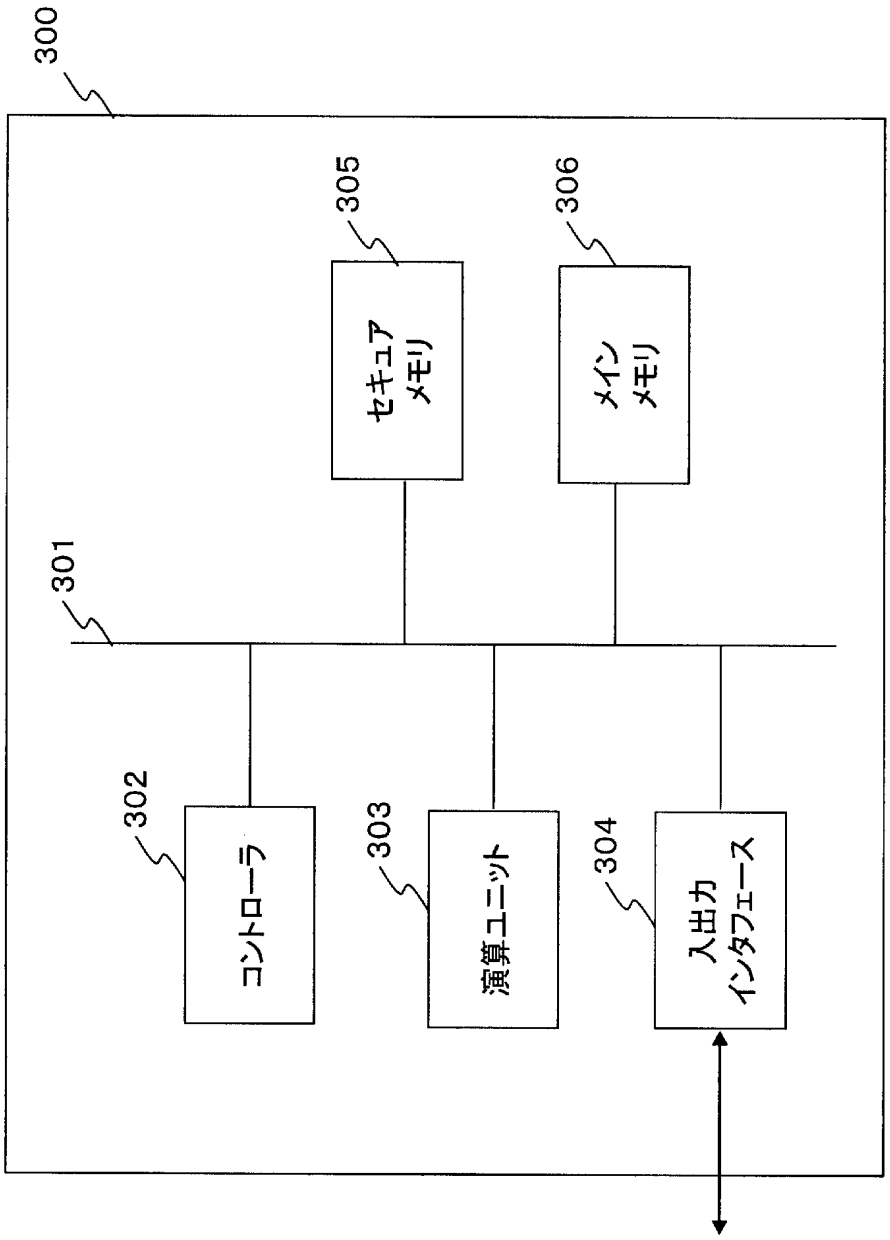
[図5]


K000
EKB復号処理
Kcon
K0010
EKB復号処理
Kcon
EKB
インデックス
暗号化キー
000
Enc(K000, Kcon)
0010
Enc(K0010, Kcon)
記録媒体

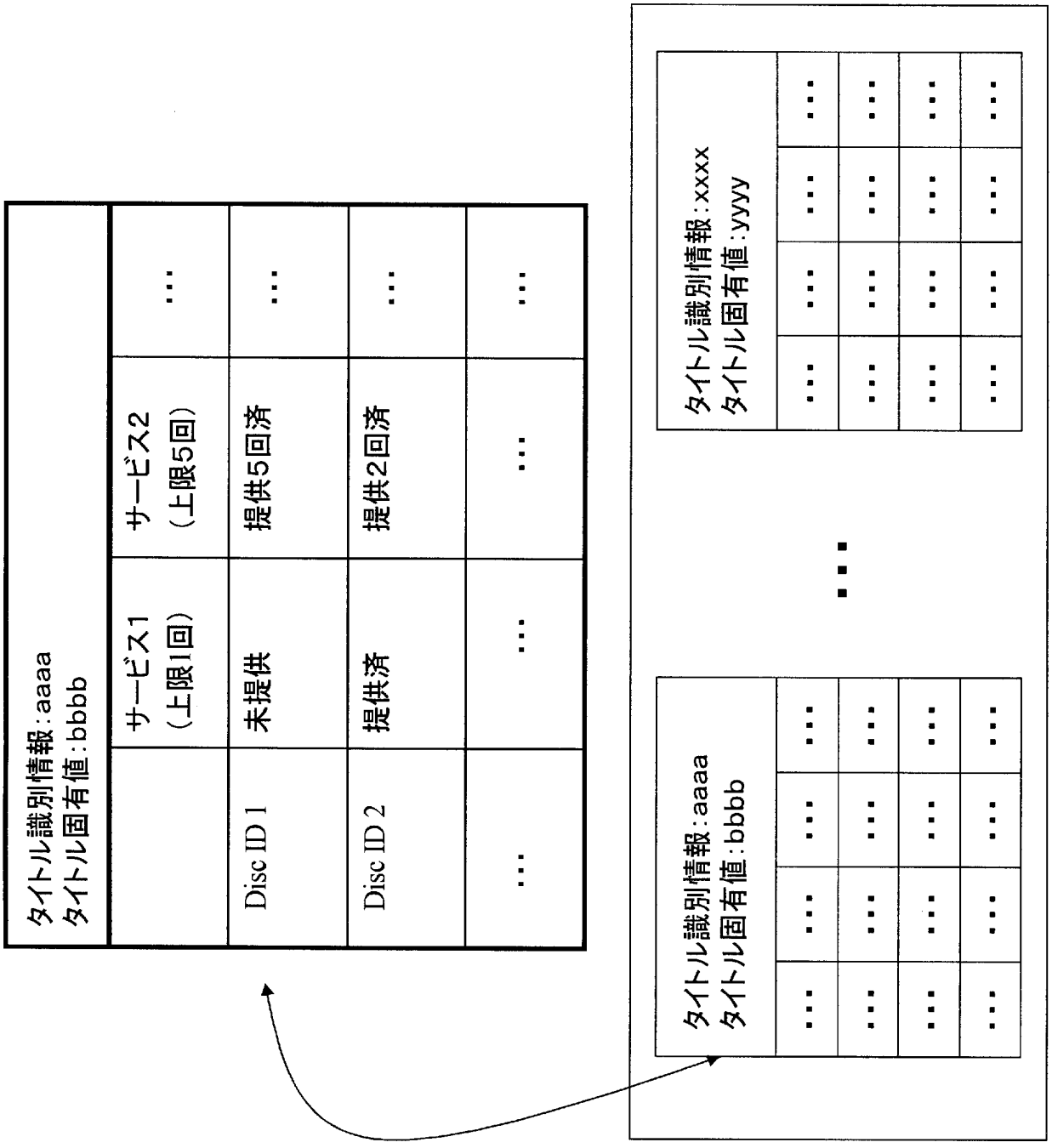
[図6]


300
サービス
提供サーバ
400
情報処理装置
(ユーザデバイス)
200
202
ディスク
製造装置
201
管理装置
(CA)
203
コンテンツ
提供装置

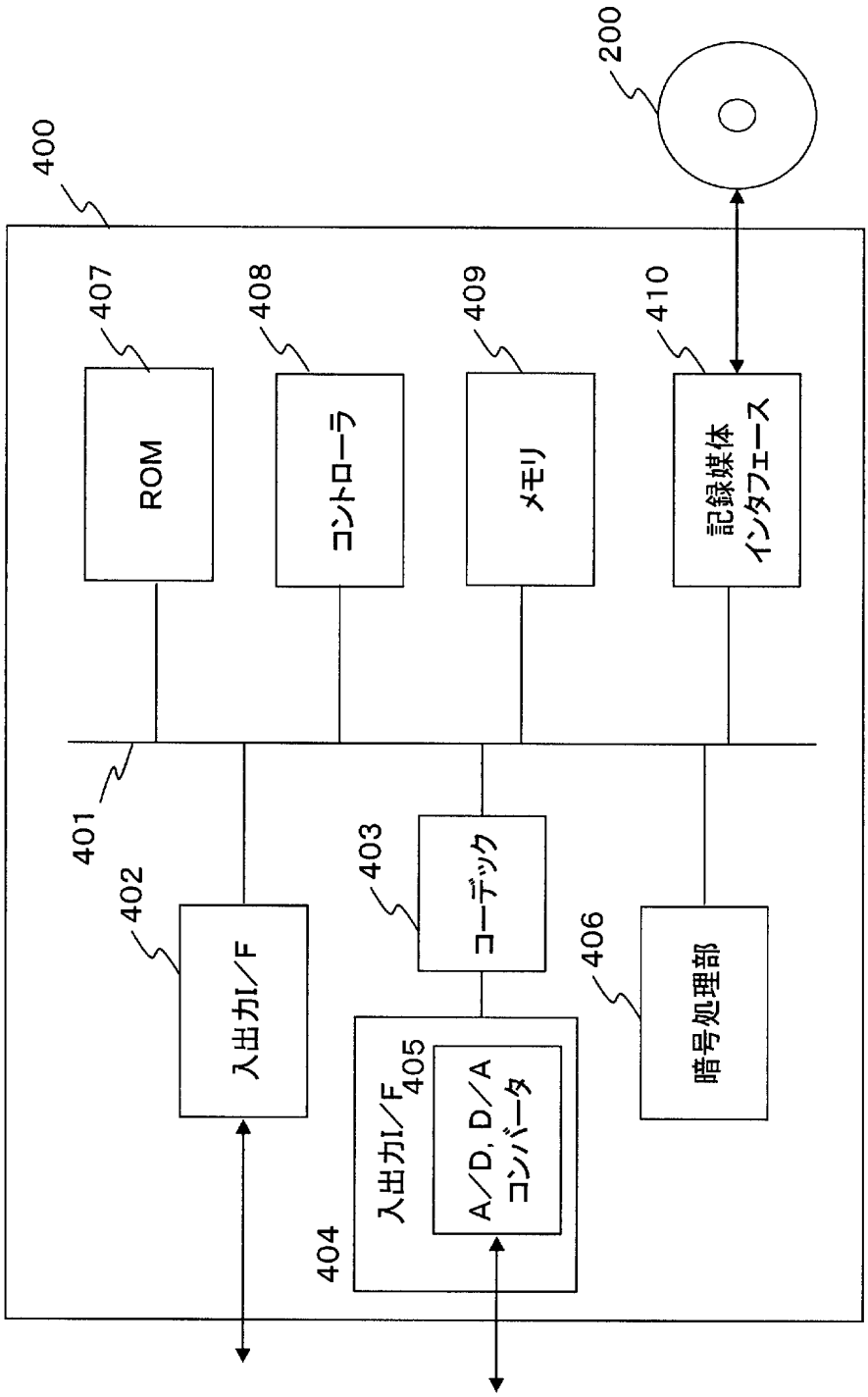
[図7]


300
305
セキュア
メモリ
306
メイン
メモリ
301
302
コントローラ
303
演算ユニット
304
入出力
インタフェース

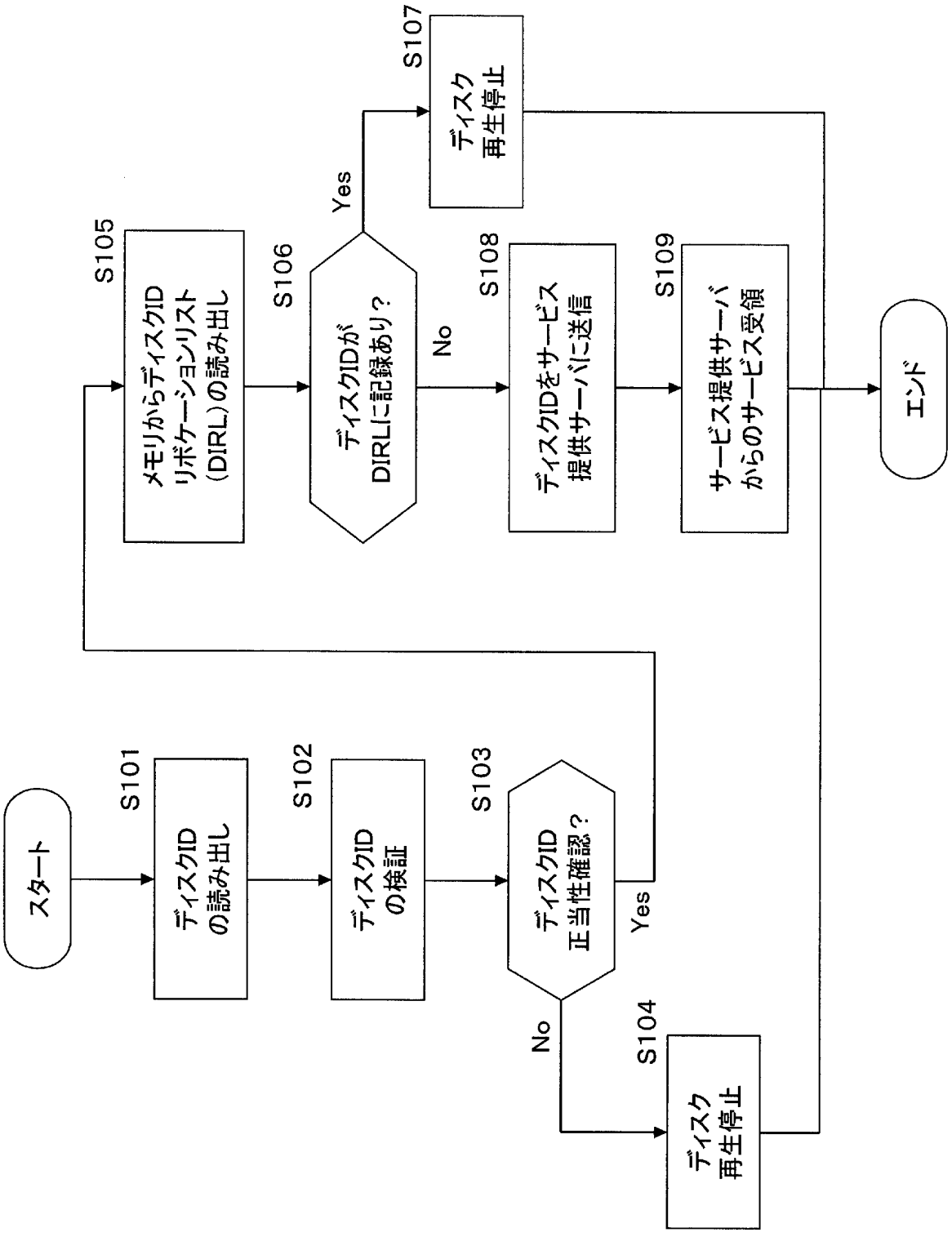
[図8]


タイトル識別情報:aaaa
タイトル固有値:bbbb
サービス1
(上限1回)
サービス2
(上限5回)
Disc ID 1
未提供
提供5回済
Disc ID 2
提供済
提供2回済
タイトル識別情報:aaaa
タイトル固有値:bbbb
タイトル識別情報:xxxx
タイトル固有値:yyyy

[図9]


200
400
407
ROM
408
コントローラ
409
メモリ
410
記録媒体
インタフェース
401
402
入出力I／F
403
コーデック
406
暗号処理部
404
入出力I／F
405
A／D, D／A
コンバータ

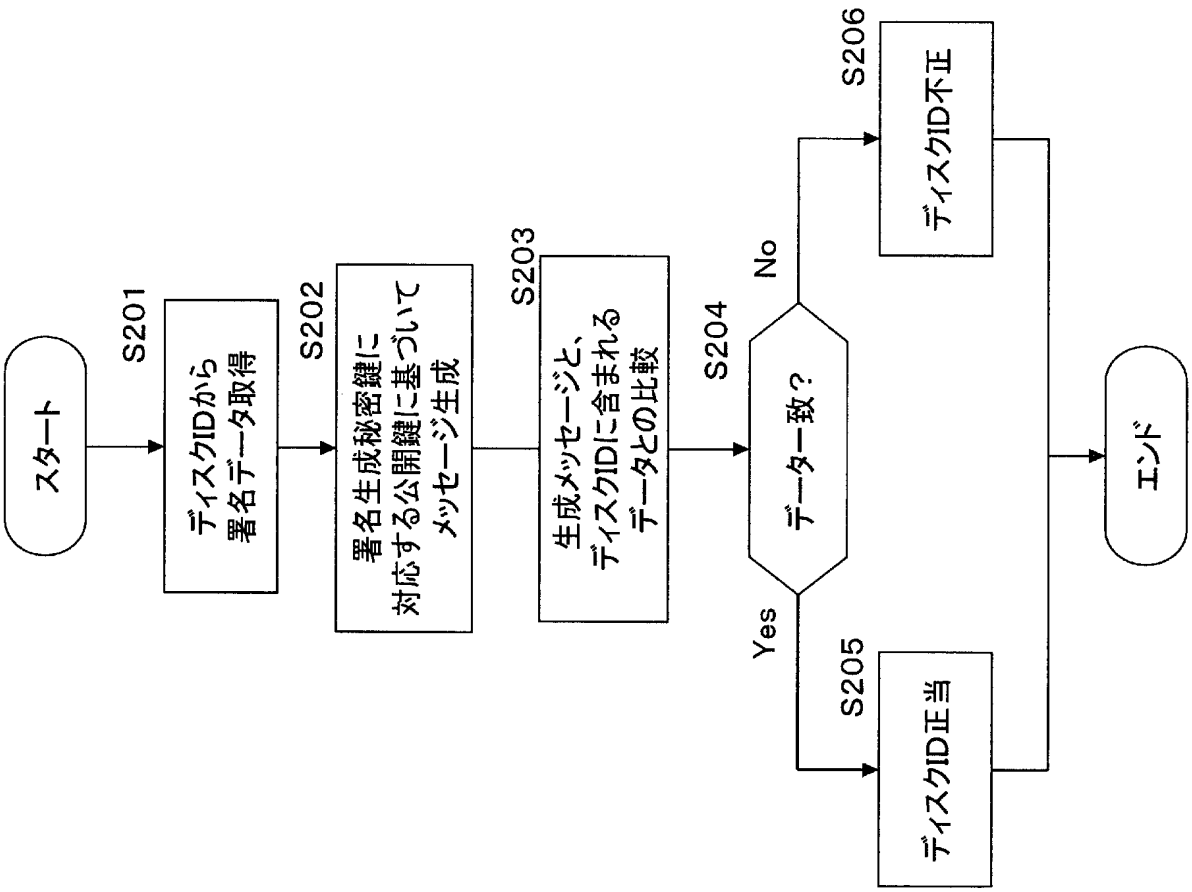
[図10]


スタート
S101
ディスクID
の読み出し
S102
ディスクID
の検証
S103
ディスクID
正当性確認？
Yes
No
S104
ディスク
再生停止
S105
メモリからディスクID
リボケーションリスト
(DIRL)の読み出し
S106
ディスクIDが
DIRLに記録あり？
Yes
No
S107
ディスク
再生停止
S108
ディスクIDをサービス
提供サーバに送信
S109
サービス提供サーバ
からのサービス受領
エンド

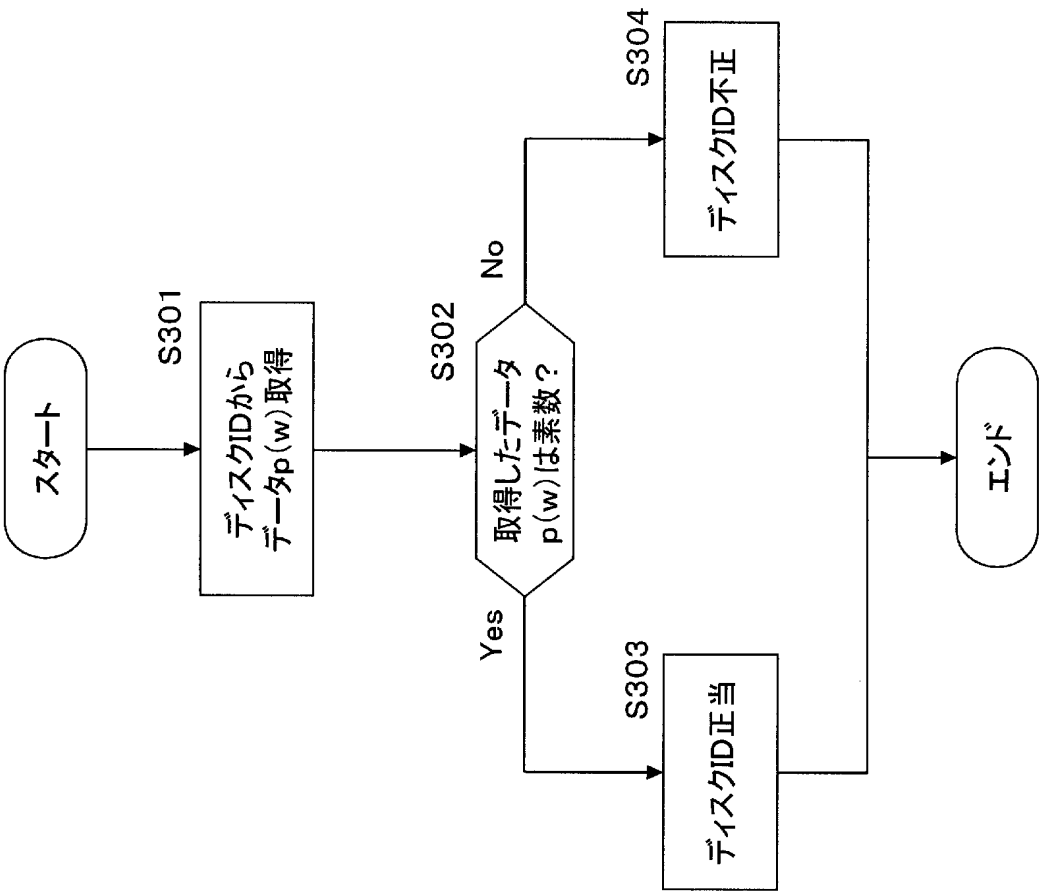
[図11]

	ディスクID	タイトル固有値	ディスク固有値
ディスクID設定例1	M, Sig(w)	M	Sig(w)
ディスクID設定例2	S, Sig(w)	S	Sig(w)
ディスクID設定例3	p(w), IDKey(w)	S	p(w) または、IDKey(w)
ディスクID設定例4	e(w), I(w)	S	e(w) または、I(w)
ディスクID設定例5	Σw	S	e(w)
ディスクID設定例6	p(w), IDKey(w)	S	p(w)

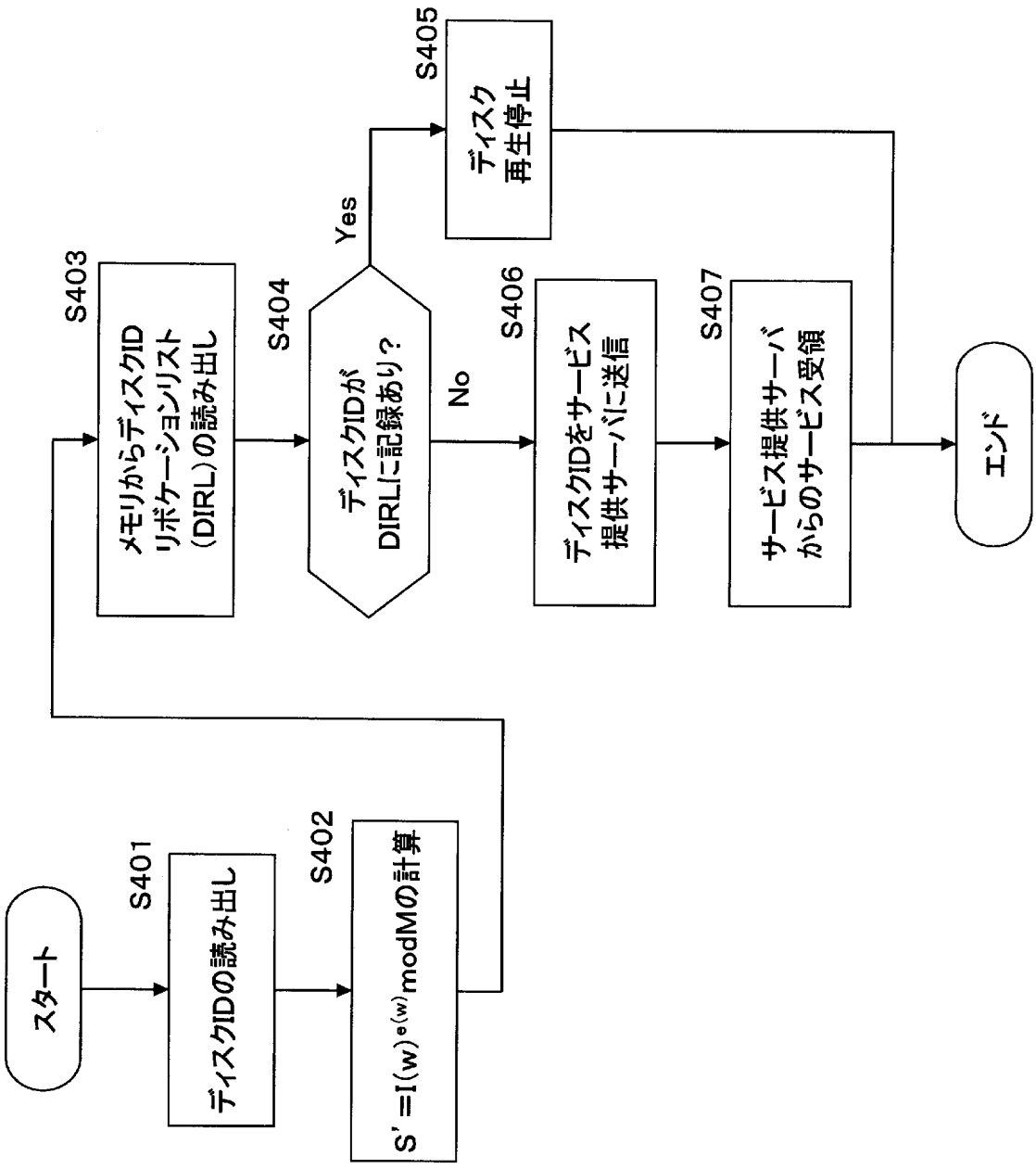
[図12]


スタート
S201
ディスクIDから
署名データ取得
S202
署名生成秘密鍵に
対応する公開鍵に基づいて
メッセージ生成
S203
生成メッセージと、
ディスクIDに含まれる
データとの比較
S204
データ一致？
No
S206
ディスクID不正
Yes
S205
ディスクID正当
エンド

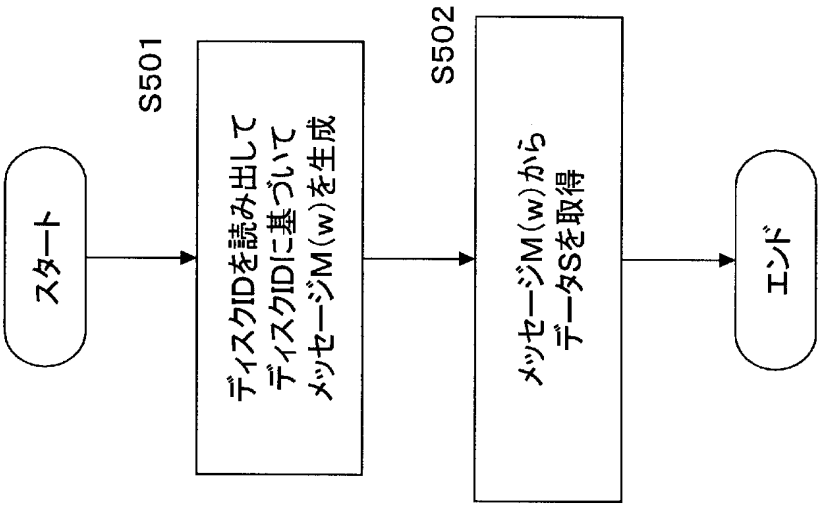
[図13]


スタート
S301
ディスクIDから
データp(w)取得
S302
取得したデータ
p(w)は素数？
No
Yes
S304
ディスクID不正
S303
ディスクID正当
エンド

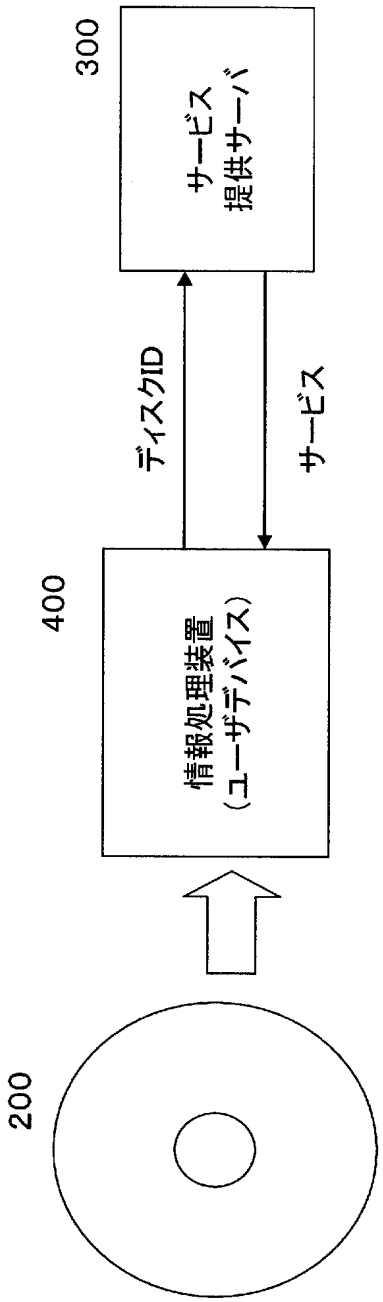
[図14]


スタート
S401
ディスクIDの読み出し
S402
S'=I(w)^e(w) modMの計算
S403
メモリからディスクID
リボケーションリスト
(DIRL)の読み出し
S404
ディスクIDが
DIRLに記録あり?
Yes
No
S405
ディスク
再生停止
S406
ディスクIDをサービス
提供サーバに送信
S407
サービス提供サーバ
からのサービス受領
エンド

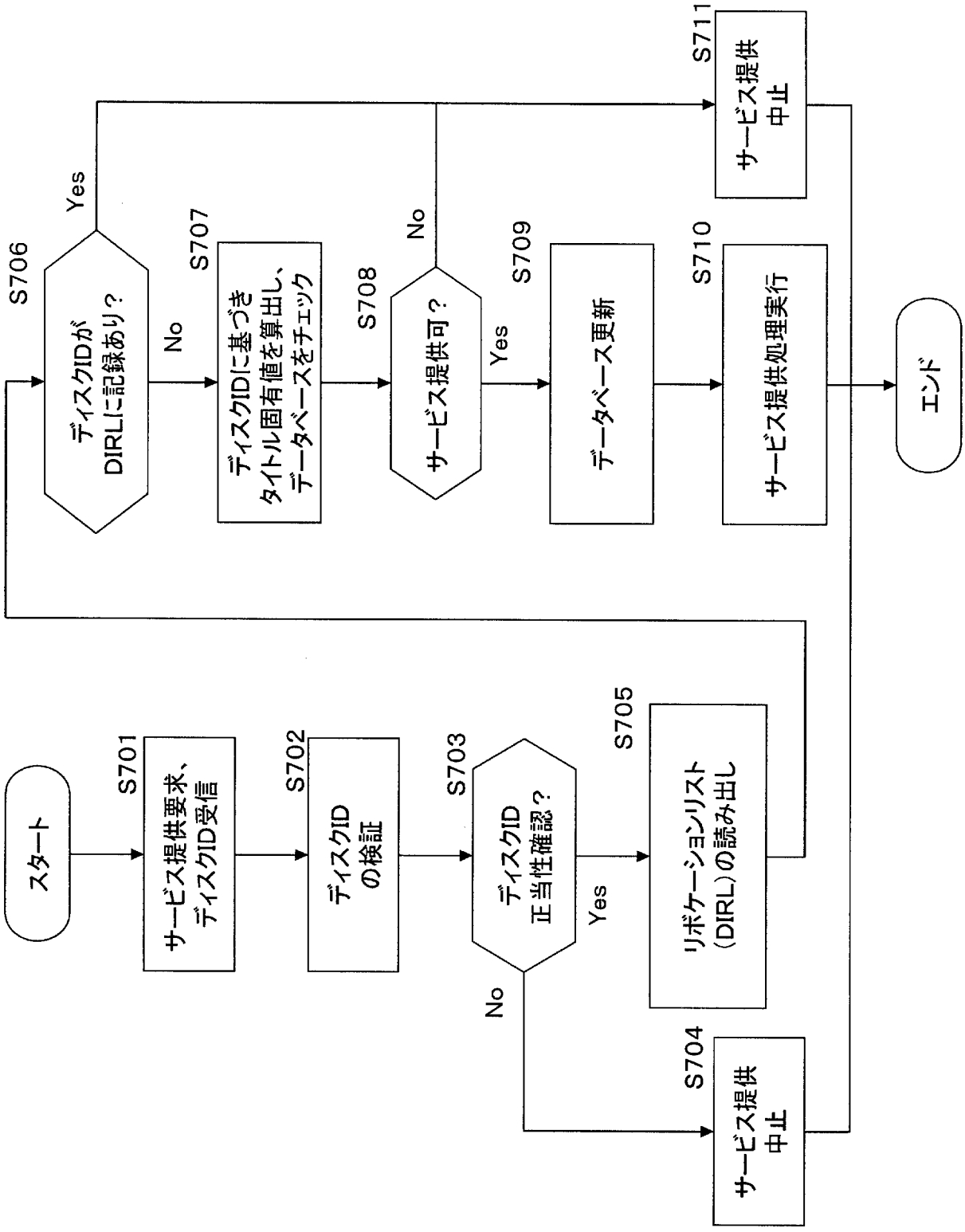
[図15]


スタート
S501
ディスクIDを読み出して
ディスクIDに基づいて
メッセージM(w)を生成
S502
メッセージM(w)から
データSを取得
エンド

[図16]



[図17]


スタート
S701
サービス提供要求、ディスクID受信
S702
ディスクIDの検証
S703
ディスクID正当性確認？
No
Yes
S704
サービス提供中止
S705
リボケーションリスト(DIRL)の読み出し
S706
ディスクIDがDIRLに記録あり？
Yes
No
S707
ディスクIDに基づきタイトル固有値を算出し、データベースをチェック
S708
サービス提供可？
No
Yes
S709
データベース更新
S710
サービス提供処理実行
S711
サービス提供中止
エンド

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2005/000497

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl[7] G06F12/14, 15/00, G11B20/10, H04L9/32

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl[7] G06F12/14, 15/00, G11B20/10, H04L9/32

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Jitsuyo Shinan Koho 1922-1996 Jitsuyo Shinan Toroku Koho 1996-2005
Kokai Jitsuyo Shinan Koho 1971-2005 Toroku Jitsuyo Shinan Koho 1994-2005

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	JP 2002-189801 A (Sony Corp.), 05 July, 2002 (05.07.02), All pages; all drawings; particularly, Par. Nos.	1,2,4-7, 9-12,14-17, 19-22
Y	[0060] to [0065] & US 2002/0099661 A1	3,8,13,18
X	WO 2002/086859 A1 (Sony Corp.), 31 October, 2002 (31.10.02), All pages; all drawings; particularly, pages	1,2,4-7, 9-12,14-17, 19-22
Y	10 to 11; Fig. 10 & US 2003/0158950 A1	3,8,13,18

☒ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
19 April, 2005 (19.04.05)	17 May, 2005 (17.05.05)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

Form PCT/ISA/210 (second sheet) (January 2004)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2005/000497

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 2002-132587 A (Sony Corp.), 10 May, 2002 (10.05.02), All pages; all drawings (Family: none)	3,8,13,18
Y	JP 2002-133767 A (Sony Corp.), 10 May, 2002 (10.05.02), All pages; all drawings (Family: none)	3,8,13,18

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２００５／０００４９７

Ａ．・発明の属する分野の分類（国際特許分類（ＩＰＣ））

Int.Cl.[7]　G06F12/14, 15/00, G11B20/10, H04L9/32

Ｂ．　調査を行った分野

調査を行った最小限資料（国際特許分類（ＩＰＣ））

Int.Cl.[7]　G06F12/14, 15/00, G11B20/10, H04L9/32

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	１９２２－１９９６年
日本国公開実用新案公報	１９７１－２００５年
日本国実用新案登録公報	１９９６－２００５年
日本国登録実用新案公報	１９９４－２００５年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

Ｃ．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
X	JP 2002-189801 A（ソニー株式会社）2002.07.05, 全頁、全図、特に【００６０】－【００６５】段落 & US 2002/0099661 A1	1, 2, 4-7, 9-12, 14-17, 19-22
Y		3, 8, 13, 18

☑ Ｃ欄の続きにも文献が列挙されている。　☐ パテントファミリーに関する別紙を参照。

＊　引用文献のカテゴリー
「Ａ」特に関連のある文献ではなく、一般的技術水準を示すもの
「Ｅ」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「Ｌ」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「Ｏ」口頭による開示、使用、展示等に言及する文献
「Ｐ」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「Ｔ」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「Ｘ」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Ｙ」特に関連のある文献であって、当該文献と他の１以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「＆」同一パテントファミリー文献

国際調査を完了した日 １９．０４．２００５	国際調査報告の発送日 17.05.2005
国際調査機関の名称及びあて先 日本国特許庁（ＩＳＡ／ＪＰ） 郵便番号１００－８９１５ 東京都千代田区霞が関三丁目４番３号	特許庁審査官（権限のある職員）　５Ｎ　３０４４ 高橋　克 電話番号　０３－３５８１－１１０１　内線　３５８６

様式ＰＣＴ／ＩＳＡ／２１０（第２ページ）（２００４年１月）

Ｃ（続き）．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
X	WO 2002/086859 A1（ソニー株式会社）2002.10.31，全頁、全図、特に第10-11頁、第10図 & US 2003/0158950 A1	1, 2, 4-7, 9-12, 14-17, 19-22
Y		3, 8, 13, 18
Y	JP 2002-132587 A（ソニー株式会社）2002.05.10，全頁、全図（ファミリーなし）	3, 8, 13, 18
Y	JP 2002-133767 A（ソニー株式会社）2002.05.10，全頁、全図（ファミリーなし）	3, 8, 13, 18